网络互联技术教程

余智豪　何志敏　马莉　编著

清华大学出版社

网络互联技术教程

余智豪　何志敏　马　莉　编著

清华大学出版社
北　京

内 容 简 介

本书技术先进，内容新颖，图文并茂，是基于 IPv4 和 IPv6 的全新的网络互联技术的教程。本书除了全面分析传统的 IPv4 路由技术外，还详细阐述了 IPv6 路由技术，深入、全面、系统地剖析了 Cisco 路由器的系统结构、工作原理、关键技术、操作命令和典型的配置实例，以直观的插图和详尽的文字来说明 Cisco 路由器的设计、部署、配置和调试的具体步骤。本书的主要内容包括网络互联技术概论、网络互联设备、路由器技术基础、路由器的基本配置、静态路由、RIP、OSPF 协议、EIGRP、访问控制列表和 IPv6 过渡技术等。

本书配备了教学 PPT、复习思考题、模拟试题和配置实例的 Packet Tracer 源文件，可以作为高等院校网络工程专业、计算机科学专业、通信专业及相关专业的本科生和大专生的教材，也可作为网络工程师或准备参加 CCNA 认证考试人员的参考书。

图书在版编目(CIP)数据

网络互联技术教程/余智豪，何志敏，马莉编著．—北京：清华大学出版社，2019
ISBN 978-7-302-50164-0

Ⅰ．①网…　Ⅱ．①余…　②何…　③马…　Ⅲ．①互联网络－教材　Ⅳ．①TP393.4

中国版本图书馆 CIP 数据核字(2018)第 112380 号

责任编辑：刘向威　常建丽
封面设计：文　静
责任校对：梁　毅
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：三河市君旺印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16　　**字　　数**：391 千字
版　　次：2019 年 1 月第 1 版　　**印　　次**：2019 年 1 月第1 次印刷
印　　数：1～1500
定　　价：49.00 元

产品编号：074686-01

前言

PREFACE

本书由多年从事计算机网络技术教学工作，并具有丰富的网络工程实践经验和大学教材编写经验的教师合作编写而成。编者根据多年的教学经验和学生的认知规律，精心组织教学内容，力争理论和实践相结合，深入浅出，循序渐进，通俗易懂，从网络体系结构、标准、协议、安全等方面对网络互联技术进行探讨，以便让读者对网络互联技术的发展和演变有比较深入的领悟和理解。

如今，国际互联网早已风靡全球，人们的生活和工作都已经离不开网络技术。但是，由于国际互联网的广泛应用，基于 IPv4 的网络地址即将枯竭，极大地阻碍了国际互联网的发展，由此产生了新一代的 IPv6 技术。毫无疑问，IPv6 取代 IPv4 是一种必然的趋势，因此，让学生同时掌握 IPv4 和 IPv6 技术，是计算机网络技术教学的当务之急。

路由器是计算机网络的核心设备，它通过光纤、卫星等通信线路将分散在世界各地的大大小小的城域网、局域网中的各种服务器和计算机互相连接在一起，组成贯穿全球的国际互联网。在网络体系结构中，基于路由技术的"网络互联技术"已经发展成为一个重要的技术分支，与"计算机网络""交换机原理""TCP/IP 技术""网络安全技术""接入网技术"等计算机网络技术课程并驾齐驱，共同构成现代网络工程技术体系。

一直以来，"网络互联技术"都是计算机网络工程专业的核心课程之一。通过这门课程的学习，学生可以系统地学习路由器和交换机的工作原理与配置知识。对于从事网络规划、设计和管理的网络工程技术人员来说，这些都是必须掌握的专业理论知识和实际操作技能。

"网络互联技术"课程教材应该包含计算机网络的体系结构、技术标准、各种路由技术的工作原理、分类和特点、适用环境、网络配置管理等主要内容。虽然专门讨论路由技术的大学教材已经较多，但是这些教材除了介绍传统的 IPv4 路由技术外，极少专门论述 IPv6 路由技术。随着国际互联网的普及，各种 IPv6 路由技术日新月异，不断涌现和发展，因此，该课程教材有必要与时俱进。与此同时，深入、详细、系统地分析和论述各种基于 IPv6 的网络互联技术，也给从事计算机网络工程技术的教学和科学研究提出了新的要求。因此，为了全面系统地介绍网络互联技术，满足网络工程专业教学和社会生产实践的需要，培养社会急需的计算机网络工程专业技术人才，我们编写了本书。

本书的主要特点是强调实用性和先进性，力求全面、客观地分析和论述网络互联技术的基本概念、基本原理；为了保持教材内容的先进性，书中涉及了各种典型的路由技术，全书共 10 章，各章的主要内容如下：

第 1 章为网络互联技术概论，主要介绍协议与分层、OSI 参考模型、TCP/IP 参考模型、IPv4、IPv6 等基本概念。

第 2 章为网络互联设备，主要介绍各种网络传输介质、物理层设备、数据链路层设备、网

络层设备和应用层设备。

第3章为路由器技术基础，主要介绍路由器的硬件结构、路由器的软件、路由器的启动过程、高端路由器、路由表、直连路由、静态路由、动态路由和管理距离等基础知识。

第4章为路由器的基本配置，主要介绍iOS、网络设备的配置方式、配置超级终端、路由器的配置向导、路由器的工作模式、路由器的常用命令、配置路由器IP地址的基本原则、iOS的备份、恢复与升级。

第5章为静态路由，主要介绍基本的IPv4静态路由配置、更复杂的IPv4静态路由配置、汇总IPv4静态路由、IPv4默认静态路由、IPv4浮动静态路由、负载均衡、配置IPv6静态路由和默认路由等知识。

第6章为RIP，主要介绍距离矢量路由协议、距离矢量路由算法、RIPv1报文格式、RIP的定时器、各种版本RIP的配置与管理等知识。

第7章为OSPF协议，主要介绍OSPF协议的工作原理、报文、分层结构、工作过程、各种版本OSPF协议的配置与管理等知识。

第8章为EIGRP，主要介绍EIGRP概述、EIGRP的工作原理、各种版本EIGRP的配置与管理等知识。

第9章为访问控制列表，主要介绍访问控制列表的工作原理、访问控制列表的应用、访问控制列表的类型、访问控制列表的配置。

第10章为IPv6过渡技术，主要介绍双协议栈技术、隧道技术、协议转换技术等知识。

由于本书涉及的知识面较广，新技术发展迅速，因此资料更新较快，编写的工作量和难度都比较大。在深入研讨、反复磋商确定编写大纲的基础上，由佛山科学技术学院的多位教师共同合作编写。其中，第1～6章、第8章和第9章由余智豪老师编写；第7章由何志敏老师编写；第10章由马莉老师编写。全书由余智豪老师统稿及修改；周灵教授、李娅副教授认真审阅了本书的书稿；张德丰教授对书稿提出了许多宝贵意见。此外，在本书的编写过程中，还得到了许多专家和同行的热心帮助和指导，在此一并致以感谢！

由于编者水平所限，本书疏漏和不当之处难以避免，希望读者不吝指正。

编　者

2018年1月于佛山科学技术学院

目录

CONTENTS

第 1 章　网络互联技术概论 …… 1

1.1　协议与分层 …… 1

1.1.1　网络协议的 3 个要素 …… 1

1.1.2　网络的分层结构 …… 1

1.1.3　网络分层的原则 …… 2

1.2　OSI 参考模型 …… 2

1.2.1　OSI 参考模型的概念 …… 2

1.2.2　OSI 参考模型各层的功能 …… 4

1.3　TCP/IP 参考模型 …… 5

1.3.1　TCP/IP 参考模型简介 …… 5

1.3.2　OSI 参考模型与 TCP/IP 参考模型的比较 …… 7

1.4　IPv4 …… 8

1.4.1　IPv4 地址的概念 …… 8

1.4.2　IPv4 简介 …… 8

1.4.3　IPv4 报文格式 …… 9

1.4.4　IPv4 的不足之处 …… 11

1.5　IPv6 …… 11

1.5.1　IPv6 地址的表示方法 …… 11

1.5.2　IPv6 的地址类型 …… 12

1.5.3　IPv6 的核心协议 …… 13

1.5.4　IPv6 报文格式 …… 14

1.6　本章总结 …… 16

复习思考题 …… 17

第 2 章　网络互联设备 …… 18

2.1　网络传输介质 …… 18

2.1.1　连接器 …… 18

2.1.2　双绞线 …… 19

2.1.3　同轴电缆 …… 20

2.1.4　光纤 …… 20

2.1.5　无线传输介质 …… 21

2.2　物理层设备 …… 22

2.2.1　中继器 …… 22

2.2.2　集线器 …… 22

2.2.3 无线接入点 …… 24
2.3 数据链路层设备 …… 25
2.3.1 网卡 …… 25
2.3.2 网桥 …… 28
2.3.3 交换机 …… 30
2.4 网络层设备 …… 32
2.5 应用层设备 …… 35
2.5.1 服务器 …… 35
2.5.2 防火墙 …… 36
2.6 本章总结 …… 37
复习思考题 …… 38
第3章 路由器技术基础 …… 40
3.1 认识路由器 …… 40
3.2 路由器的硬件结构 …… 41
3.3 路由器的软件 …… 43
3.4 路由器的启动过程 …… 45
3.5 高端路由器 …… 46
3.6 路由表 …… 47
3.7 直连路由 …… 48
3.8 静态路由 …… 49
3.9 动态路由 …… 50
3.9.1 动态路由与静态路由的比较 …… 50
3.9.2 静态路由的优缺点 …… 51
3.9.3 动态路由的优缺点 …… 52
3.9.4 动态路由协议的分类 …… 52
3.10 管理距离 …… 54
3.11 本章总结 …… 55
复习思考题 …… 56
第4章 路由器的基本配置 …… 58
4.1 互联网操作系统 …… 58
4.2 网络设备的配置方式 …… 58
4.3 配置超级终端 …… 60
4.3.1 在 Windows XP 系统中配置超级终端 …… 60
4.3.2 在 Windows 7 系统中配置超级终端 …… 61
4.4 路由器的配置向导 …… 62
4.5 路由器的工作模式 …… 62
4.6 路由器的常用命令 …… 64
4.7 配置路由器 IP 地址的基本原则 …… 70
4.8 iOS 的备份、恢复和升级 …… 71
4.9 本章总结 …… 73
复习思考题 …… 74

第 5 章　静态路由 …… 76
5.1　基本的 IPv4 静态路由配置 …… 76
5.2　更复杂的 IPv4 静态路由配置 …… 80
5.3　汇总 IPv4 静态路由 …… 83
5.4　IPv4 默认静态路由 …… 86
5.5　IPv4 浮动静态路由 …… 87
5.6　负载均衡 …… 89
5.7　配置 IPv6 静态路由和默认路由 …… 90
5.8　本章总结 …… 94
复习思考题 …… 95
第 6 章　RIP …… 96
6.1　RIP 的发展简史 …… 96
6.2　距离矢量路由协议 …… 97
6.3　距离矢量路由算法 …… 98
6.4　路由环路及解决方法 …… 102
6.4.1　路由环路产生的原因 …… 103
6.4.2　路由环路的解决方法 …… 103
6.5　RIPv1 报文格式 …… 105
6.6　RIP 的计时器 …… 106
6.7　RIPv1 的配置与管理 …… 107
6.8　RIPv2 的配置与管理 …… 110
6.8.1　RIPv1 与 RIPv2 的特性比较 …… 110
6.8.2　RIPv2 的配置与管理 …… 111
6.9　RIPng 的配置与管理 …… 114
6.9.1　RIPng 的工作原理 …… 114
6.9.2　RIPng 与 RIPv1、RIPv2 的比较 …… 115
6.9.3　RIPng 配置与管理 …… 116
6.10　本章总结 …… 119
复习思考题 …… 120
第 7 章　OSPF 协议 …… 122
7.1　OSPF 协议的工作原理 …… 122
7.2　OSPF 报文 …… 123
7.2.1　OSPF 报头格式 …… 123
7.2.2　OSPF 正文格式 …… 124
7.3　OSPF 分层结构 …… 128
7.4　OSPF 协议的工作过程 …… 129
7.5　OSPF 配置与管理 …… 132
7.5.1　OSPFv2 配置与管理 …… 132
7.5.2　OSPFv3 配置与管理 …… 135
7.6　本章总结 …… 138
复习思考题 …… 140

第 8 章 EIGRP …… 141
8.1 EIGRP 概述 …… 141
8.1.1 IGRP 与 EIGRP …… 141
8.1.2 EIGRP 的优点 …… 142
8.1.3 EIGRP 与 OSPF 协议的比较 …… 142
8.2 EIGRP 的工作原理 …… 143
8.2.1 可靠传输协议 …… 143
8.2.2 扩散更新算法的相关术语 …… 143
8.2.3 实现路由快速收敛的关键 …… 144
8.2.4 路由计算方法 …… 144
8.2.5 EIGRP 数据包 …… 145
8.2.6 修改计时器的方法 …… 146
8.2.7 解决环路问题 …… 146
8.2.8 DUAL 有限状态机 …… 147
8.3 EIGRP 的配置和管理 …… 148
8.3.1 EIGRP 配置命令 …… 148
8.3.2 EIGRP 调试命令 …… 149
8.3.3 EIGRP 配置实例 …… 149
8.4 支持 IPv6 的 EIGRP …… 152
8.4.1 支持 IPv6 的 EIGRP 的特点 …… 152
8.4.2 配置 EIGRPv6 的命令 …… 152
8.4.3 测试 EIGRPv6 的命令 …… 152
8.4.4 EIGRPv6 的配置实例 …… 153
8.5 本章总结 …… 157
复习思考题 …… 159
第 9 章 访问控制列表 …… 161
9.1 访问控制列表概述 …… 161
9.1.1 访问控制列表的功能 …… 161
9.1.2 建立访问控制列表的作用 …… 162
9.2 访问控制列表的工作原理 …… 163
9.3 访问控制列表的分类和原则 …… 164
9.3.1 访问控制列表的分类 …… 164
9.3.2 定义 ACL 时应遵循的原则 …… 165
9.4 配置标准访问控制列表 …… 166
9.5 用标准 ACL 限制虚拟终端的访问 …… 171
9.6 配置扩展访问控制列表 …… 172
9.7 配置命名的访问控制列表 …… 174
9.7.1 命名 ACL 与编号 ACL 的区别 …… 174
9.7.2 配置命名 ACL 的语法格式 …… 175
9.8 配置基于时间的访问控制列表 …… 177
9.9 配置 IPv6 访问控制列表 …… 178
9.9.1 创建 IPv6 访问控制列表 …… 178
9.9.2 在接口上应用 IPv6 访问控制列表 …… 178
9.9.3 配置标准 IPv6 访问控制列表 …… 178

9.9.4　配置扩展 IPv6 访问控制列表 …… 182
9.10　本章总结 …… 185
复习思考题 …… 186
第 10 章　IPv6 过渡技术 …… 187
10.1　过渡技术概述 …… 187
10.2　双协议栈技术 …… 188
10.2.1　双协议栈技术简介 …… 188
10.2.2　双协议栈关键技术 …… 189
10.2.3　ICMPv6 简介 …… 190
10.2.4　邻居发现协议简介 …… 190
10.2.5　支持 IPv6 的 DNS 简介 …… 191
10.2.6　在路由器上配置双协议栈 …… 192
10.3　隧道技术 …… 193
10.3.1　手动配置隧道 …… 194
10.3.2　GRE 隧道 …… 194
10.3.3　自动配置的兼容隧道 …… 195
10.3.4　6over4 隧道 …… 195
10.3.5　6to4 隧道 …… 196
10.3.6　6RD 隧道 …… 196
10.3.7　ISATAP 隧道 …… 197
10.3.8　Teredo 隧道 …… 198
10.3.9　隧道代理技术 …… 198
10.3.10　隧道配置示例 …… 199
10.4　协议转换技术 …… 203
10.4.1　NAT-PT …… 203
10.4.2　NAT64 …… 204
10.4.3　NAT64 配置示例 …… 205
10.5　本章总结 …… 208
复习思考题 …… 209
附录 A　思科 Packet Tracer 7.0 使用简介 …… 212
A.1　Packet Tracer 7.0 安装方法 …… 212
A.2　将工作界面修改为中文 …… 216
A.3　Packet Tracer 7.0 的工作区域 …… 219
A.4　布置网络设备 …… 220
A.5　连接网络设备 …… 220
A.6　配置网络设备 …… 221
A.7　模拟模式 …… 226
A.8　Packet Tracer 的帮助文件 …… 227
附录 B　模拟试题 …… 228
B.1　模拟试题一 …… 228
B.2　模拟试题二 …… 232
附录 C　常用英文缩写对照表 …… 236
参考文献 …… 245

第1章 网络互联技术概论

CHAPTER 1

网络互联是指将两个以上的通信网络通过一定的技术与方法，用一种或多种网络通信设备相互连接起来，构成更大的网络系统。网络互联的目的是实现不同网络中的用户可以互相通信、共享软件和数据等。

本章首先介绍计算机网络协议的基本概念和计算机网络分层的思想，接着介绍 OSI 参考模型和 TCP/IP 模型，最后分别介绍 IPv4、IPv6 的基本原理。

1.1 协议与分层

在计算机网络的各种设备之间要实现数据的交换，就必须遵守一些事先约定的规则。这些规则明确规定了所交换的数据的格式，还要解决同步问题。这里所说的同步不是狭义的同步(同频率或同相位)，而是广义的同步，即在下一条件下应当发生什么事件，因此同步包含时序的意思。

1.1.1 网络协议的3个要素

为进行计算机网络中的数据交换而建立的规则、标准或约定称为网络协议(network protocol)。网络协议简称为协议。准确地说，网络协议主要由以下3个要素组成：

(1) 语法：即数据与控制信息的结构或格式。

(2) 语义：即需要发出何种控制信息，完成何种动作和做出何种响应。

(3) 同步：即事件实现顺序的详细说明。

由此可见，网络协议是计算机网络不可缺少的组成部分。实际上，只要想让连接在网络上的另一台计算机做事情(例如，在网络上发送一封电子邮件)，通信双方就都需要遵守网络协议。但是，当我们在自己的计算机上进行文件保存操作时，就不需要任何协议，除非这个文件需要保存到网络中的某个服务器上。

协议通常有两种形式：一种形式是采用便于人们阅读和理解的文字来描述；另一种形式则是使用计算机能够理解的程序代码来描述。这两种不同的形式都必须能够对网络上交换的信息做出精确的解释。

1.1.2 网络的分层结构

在网络体系结构中，用分层来实现网络的结构化设计。网络分层就是将网络结点中的数据的发送或转发、打包或拆包，控制信息的加载或拆出等工作，分别由不同的硬件和软件

模块去完成。这样可以将往来通信和网络互联这一复杂的问题变得较为简单。

在各层分别定义标准接口，使具备相同对等层的不同网络设备能实现互操作，各层之间则相对独立，一种高层协议可放在多种低层协议上运行。

在复杂的计算机网络体系结构中，划分层次是必要的。因为划分层次可以带来以下多种好处：

(1) 各层之间是独立的。某一层并不需要知道它的下一层是如何实现的，而仅仅需要知道该层通过层间的接口（即界面）所提供的服务。由于每一层只实现一种相对独立的功能，因而可将一个难以处理的复杂问题分解为若干较容易处理的、比较简单的问题。这样，整个问题的复杂程度就降低了。

(2) 灵活性好。当任何一层发生变化时（如由于技术的变化），只要层间接口关系保持不变，则在这层以上或以下的各层均不受影响。此外，对某一层提供的服务还可以进行修改。当不再需要某层提供的服务时，可以将这层取消。

(3) 结构上可分割开。各层都可以采用最合适的技术来实现。

(4) 易于实现和维护。分层结构使得实现和调试一个庞大而复杂的系统易于处理，因为整个庞大的系统已经被分解为若干相对独立的子系统。

(5) 能促进标准化工作。因为每一层的功能及其提供的服务都已有了精确的说明。

1.1.3 网络分层的原则

分层时应注意使每一层的功能明确。分层的层数不能太少，也不能太多。因为层数太少会使每一层的协议太复杂，而层数太多又会在描述和综合各层功能的系统工程任务时遇到较多的困难。通常，每一层要实现的一般功能，往往是下列的某一种功能或多种功能：

(1) 差错控制。使得和网络对端的相应层次的通信更加可靠。

(2) 流量控制。使得发送端的发送速率不会太快，以便接收端能够及时接收数据。

(3) 分段和重装。发送端将要发送的数据块划分为更小的单位，在接收端将其还原。

(4) 复用和分用。发送端几个高层会话复用一条低层的连接，在接收端再进行分用。

(5) 连接建立和释放。交换数据前先建立一条逻辑连接。数据传送结束后释放连接。

但是，分层也有一些缺点，例如有些功能会在不同的层次中重复出现，因而产生了额外开销。

我们将计算机网络的各层及其协议的集合，称为网络的体系结构。也就是说，计算机网络的体系结构就是这个计算机网络及其部件所应完成的功能的精确定义。值得注意的是，这些功能究竟是用何种硬件或软件完成的，则是一个遵循这种体系结构的实现问题。总之，体系结构是抽象的，而实现是具体的，是真正在运行的计算机硬件和软件。

1.2 OSI 参考模型

1.2.1 OSI 参考模型的概念

在计算机网络刚刚出现的时候，很多大型的计算机公司都拥有网络技术，公司内部的计算机可以相互连接，可是却不能与其他公司的计算机连接，原因是国际上并没有一个统一的计算机网络规范。因为不同厂商的计算机之间不能理解对方传输的信息，所以不能实现

互连。

国际标准化组织(International Organization for Standardization,ISO)为了使网络应用更为普及,于 1984 年推出了开放式系统互连(Open System Interconnect,OSI)参考模型。其目标就是建议所有计算机公司都使用这个规范来控制网络。这样,所有公司都有相同的规范,就能实现网络互联了。

一般称 OSI 为 OSI 参考模型。该体系结构标准定义了网络互联的 7 层框架(物理层、数据链路层、网络层、传输层、会话层、表示层和应用层),如图 1-1 所示。国际标准化组织在这一框架下进一步详细规定了每一层的功能,以实现开放系统环境中的互连性、互操作性和应用的可移植性。

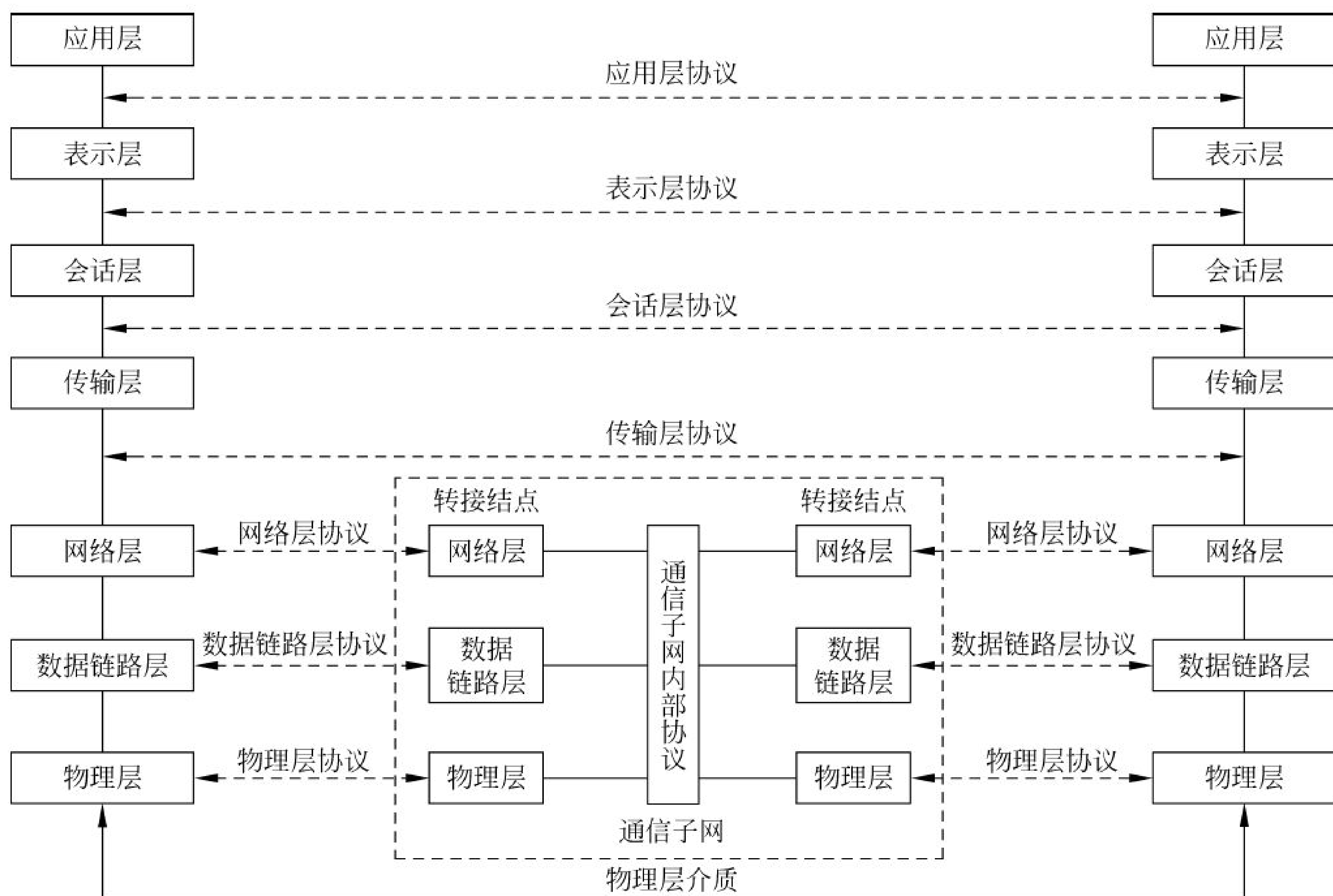


图 1-1 OSI 参考模型

OSI 参考模型明确区分了服务、接口和协议这 3 个概念。在这个逻辑的分层结构中,每一层会接受下层所提供的服务,并且向上层提供服务。接受和提供服务是通过服务访问点(Service Access Point,SAP)来实现的,而具体的服务是通过协议来实现的。

OSI 参考模型采用的方法是将整个庞大而复杂的问题划分为若干容易处理的小问题,这就是分层的体系结构方法。在 OSI 参考模型中,采用了三级抽象,即体系结构、服务定义和协议规定说明。

OSI 参考模型定义了开放系统的层次结构、层次之间的相互关系及各层可能包含的服务。它作为一个框架协调和组织各层协议的制定,也是对网络内部结构最精练的概括与描述进行整体修改。

OSI 的服务定义详细说明了各层所提供的服务。某一层的服务就是指该层向其上一层提供的一个功能模块。它通过接口提供给更高一层。各层所提供的服务与这些服务是怎么

实现的无关。同时,各种服务还定义了层与层之间的接口和各层使用的原语,但是不涉及接口是怎么实现的。

OSI 参考模型中的各种协议精确定义了应当发送什么样的控制信息,以及应当用什么样的过程来解释这个控制信息。协议的规程说明具有最严格的约束。

根据分而治之的原则,OSI 参考模型将整个通信功能划分为 7 个层次,划分原则是:

(1) 网络中的各结点都有相同的层次。

(2) 不同结点的同等层具有相同的功能。

(3) 同一结点内的相邻层之间通过接口通信。

(4) 每一层使用下层提供的服务,并向其上层提供服务。

(5) 不同结点的同等层按照协议实现对等层之间的通信。

(6) 根据功能需要进行分层,每层应当具有明确的功能。

(7) 向应用程序提供服务。

1.2.2 OSI 参考模型各层的功能

1. 物理层

物理层是 OSI 参考模型的最低层,它利用传输介质为数据链路层提供物理连接。它主要关心的是通过物理链路从一个结点向另一个结点传送比特流,物理链路可能是铜线、卫星、微波或其他的通信媒介。物理层关心的是链路的机械、电气、功能和规程特性。常用的物理层设备有网卡、集线器、中继器、调制解调器、光纤、双绞线、同轴电缆。典型的物理层协议有 RJ-45 协议(定义了以太网链路的物理层)、RS-232 协议(定义了串行链路的物理层)、工业科学医学(Industrial Scientific Medical,ISM)协议(定义了 WiFi 和蓝牙的物理层)等。

2. 数据链路层

数据链路层是为网络层提供服务的,解决两个相邻结点之间的通信问题,传送的协议数据单元称为数据帧。数据帧中包含物理地址(又称 MAC 地址)、控制码、数据及校验码等信息。该层的主要作用是通过校验、确认和反馈重发等手段,将不可靠的物理链路转换成对网络层来说无差错的数据链路。数据链路层还要协调收发双方的数据传输速率,即进行流量控制,以防止接收方因来不及处理发送方发来的高速数据而导致缓冲器溢出及线路阻塞。常用的数据链路层设备有网桥、交换机。典型的数据链路层协议有 802.2 协议、802.3 协议、HDLC 协议、帧中继(Frame Relay,FR)协议和点到点协议(Point to Point Protocol,PPP)等。

3. 网络层

网络层是为传输层提供服务的,传送的协议数据单元称为数据包或分组。该层的主要作用是解决如何使数据包通过各结点传送的问题,即通过路径选择算法(路由)将数据包送到目的地。为避免通信子网中出现过多的数据包而造成网络阻塞,需要对流入的数据包数量进行控制(拥塞控制)。当数据包要跨越多个通信子网才能到达目的地时,还要解决网际互联的问题。常用的网络层设备是路由器。典型的网络层协议是 IPv4 协议和 IPv6 协议。除此之外,还有 ICMP、IGMP 等协议。

4. 传输层

传输层的作用是为上层协议提供端到端的可靠和透明的数据传输服务,包括处理差错控制和流量控制等问题。该层向高层屏蔽了下层数据通信的细节,使高层用户看到的只是

在两个传输实体间的一条主机到主机的、可由用户控制和设定的、可靠的数据通路。传输层传送的协议数据单元称为段或报文。典型的传输层协议是 TCP 和 UDP。

5. 会话层

会话层的主要功能是管理和协调不同主机上各种进程之间的通信(对话),即负责建立、管理和终止应用程序之间的会话。会话层得名的原因是它很类似于两个实体间的会话概念。例如,一个交互的用户会话以登录到计算机开始,以注销结束。会话层传送的协议数据单元是 SPDU(会话层协议数据单元)。典型的会话层协议有 H.245,这是 H.323 协议簇中负责多媒体连接控制的协议。

6. 表示层

表示层处理流经结点的数据编码的表示方式问题,以保证一个系统的应用层发出的信息可被另一系统的应用层读出。如果有必要,该层可提供一种标准表示形式,用于将计算机内部的多种数据表示格式转换成网络通信中采用的标准表示形式。通俗地说,表示层是网络中的数据翻译官。此外,数据压缩和加密也是表示层可提供的转换功能之一。表示层传送的协议数据单元是 PPDU(表示协议数据单元)。典型的表示层协议有 ASCII 和 EBCDIC,因为它们提供的功能与 OSI 对表示层的描述相关。

7. 应用层

应用层是 OSI 中的最高层,为特定类型的网络应用提供了访问 OSI 环境的手段。应用层确定进程之间通信的性质,以满足用户的需要。应用层不仅要提供应用进程所需要的信息交换和远程操作,而且还要作为应用进程的用户代理完成一些为进行信息交换所必需的功能。它包括:文件传送访问和管理(FTAM)、虚拟终端(VT)、事务处理(TP)、远程数据库访问(RDA)、制造报文规范(MMS)、目录服务(DS)等协议;应用层能与应用程序界面沟通,以达到展示给用户的目的。在应用层中,常见的协议有 HTTP、HTTPS、FTP、TELNET、SSH、SMTP 和 POP3 等。

OSI 参考模型是一个定义良好的协议规范集,并有许多可选部分用于完成类似的任务。它定义了开放系统的层次结构、层次之间的相互关系以及各层包括的可能作为一个框架来协调和组织各层提供的服务。

OSI 参考模型仅仅是一个理论参考模型,并没有提供一个可以实现的方法,而是描述了一些概念,用来协调进程间通信标准的制定,即 OSI 参考模型并不是一个标准,而是一个在制定标准时使用的概念性框架。

1.3 TCP/IP 参考模型

1.3.1 TCP/IP 参考模型简介

TCP/IP 参考模型是早期的 ARPANET 网络和其后继的国际互联网使用的计算机网络参考模型。ARPANET 网络是由美国国防部(U.S.A Department of Defense)赞助的研究网络。ARPANET 最初通过租用的电话线连接了美国数百所大学和政府部门,后来一直发展,通过各种有线(电话线、光纤等)和无线(卫星通信、地面微波通信等)的传输方式,跨越了美国,连接遍及世界各国的计算机,成为如今拥有数十亿用户的国际互联网(Internet)。

TCP/IP 参考模型是首先由 ARPANET 使用的网络体系结构。这个体系结构在它的

两个主要协议出现以后被称为TCP/IP参考模型(TCP/IP Reference Model)。TCP/IP参考模型自下而上共分为4层：网络接口层、互联网层、传输层和应用层，如图1-2所示。

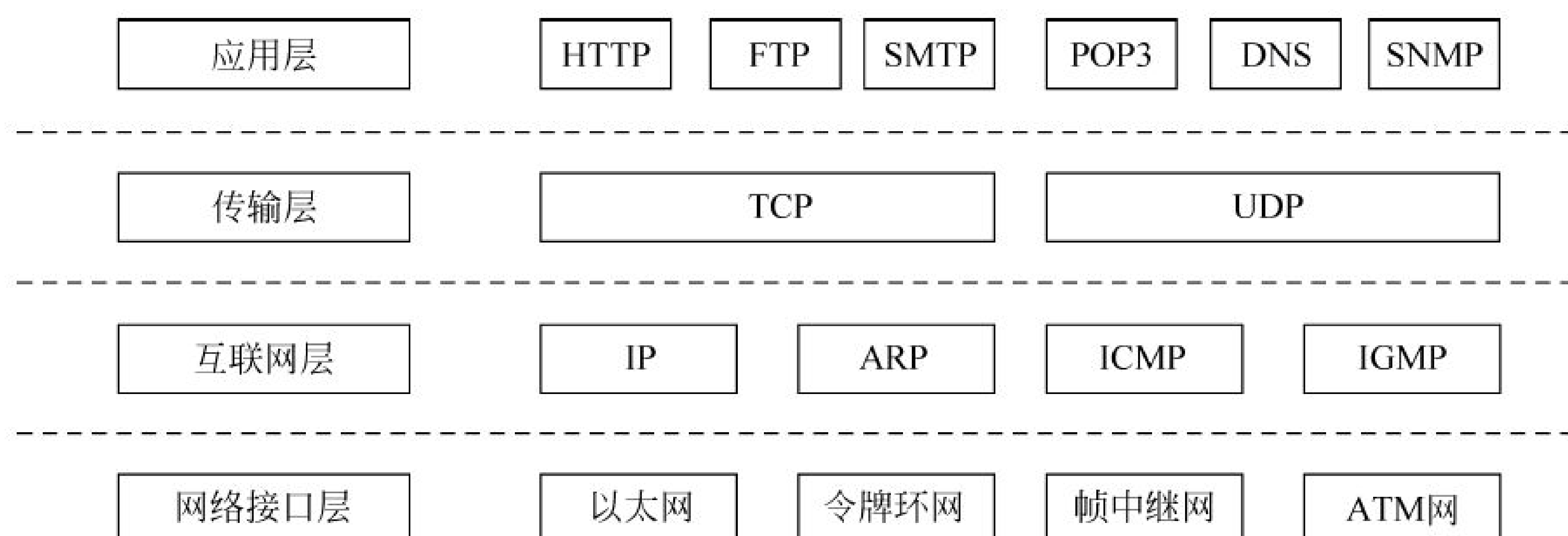


图1-2　TCP/IP参考模型

1. 网络接口层

网络接口层(Network Access Layer)在TCP/IP参考模型中并没有详细描述，只是指出主机必须使用某种协议与网络相连。

网络接口层与OSI参考模型中的物理层和数据链路层对应。网络接口层是TCP/IP与各种局域网(LAN)或广域网(WAN)的接口。

网络接口层在发送端将上层的IP数据报封装成帧后发送到网络上；当数据帧通过网络到达接收端时，该结点的网络接口层对数据帧拆封，并检查帧中包含的MAC地址。如果该地址就是本机的MAC地址或者是广播地址，则上传到网络层，否则丢弃该帧。

当使用串行线路连接主机与网络，或连接网络与网络时，例如主机通过Modem和电话线接入Internet时，则需要在网络接口层运行SLIP或PPP。

2. 互联网层

互联网层(Internet Layer)是整个体系结构的关键部分，其功能是使主机可以把分组(或称为数据包)发往任何网络，并使分组独立地传向目标。这些分组可能经由不同的网络，到达的顺序和发送的顺序也可能不同。高层如果需要顺序收发，那么就必须自行处理对分组的排序。互联网层使用因特网协议(Internet Protocol，IP)。TCP/IP参考模型的互联网层和OSI参考模型的网络层在功能上非常相似。

互联网层是将整个网络体系结构贯穿在一起的关键层。该层的任务是，允许主机将分组发送到任何网络上，并且让这些分组独立地到达目标端。

这些分组到达的顺序可能与它们被发送时的顺序不同。在这种情况下，如果有必要按原来的顺序重新排列，则由高层负责重新排列这些分组的任务。

互联网层定义了正式的分组格式和协议，该协议称为IP。互联网层的任务是将IP分组传送到它们该去的地方。

3. 传输层

传输层(Transport Layer)使源端和目的端机器上的对等实体可以进行会话。传输层定义了两个端到端的协议：传输控制协议(Transmission Control Protocol，TCP)和用户数据报协议(User Datagram Protocol，UDP)。TCP是面向连接的协议，提供可靠的报文传输和对上层应用的连接服务。为此，除了基本的数据传输外，TCP还有可靠性保证、流量控

制、多路复用、优先权和安全性控制等功能。UDP是面向无连接的不可靠传输的协议，主要用于不需要TCP的排序和流量控制等功能的应用程序。

传输控制协议是面向连接的、可靠的、端到端的、基于字节流的传输协议。TCP不支持多播(multicast)和广播(broadcast)。TCP连接是基于字节流的，而不是消息流，消息的边界在端到端的传输中不能得到保留；对于应用程序发来的数据，TCP可以立即发送，也可以缓存一段时间，以便一次发送更多的数据。为了强迫数据发送，可以使用PUSH标记；对于紧急数据(urgent data)，可以使用URGENT标记。

用户数据报协议提供了不可靠的无连接传输服务。它使用IP携带报文，但增加了对给定主机上多个目标进行区别的能力。UDP没有确认机制，不对报文排序，没有超时机制，没有反馈机制控制流量。使用UDP的应用程序要承担可靠性方面的全部工作。

4. 应用层

应用层(Application Layer)是TCP/IP参考模型的最高层。应用层直接和应用程序接口连接，并提供常见的网络应用服务。

在TCP/IP参考模型中，把原来OSI参考模型最上面的3层(即应用层、表示层和会话层)合并为应用层。应用层是直接为应用进程提供服务的。其作用是在实现多个系统应用进程相互通信的同时，完成一系列业务处理所需的服务。其服务元素分为两类：公共应用服务元素(CASE)和特定应用服务元素(SASE)。

CASE提供最基本的服务，成为应用层中任何用户和任何服务元素的用户，主要为应用进程通信、分布系统实现提供基本的控制机制。SASE则要满足一些特定服务，如文卷传送、访问管理、作业传送、银行事务、订单输入等。这些将涉及虚拟终端、作业传送与操作、文卷传送及访问管理、远程数据库访问、图形核心系统和开放系统互连管理等。

应用层包含所有的高层协议，包括虚拟终端协议(TELecommunications NETwork，TELNET)、文件传输协议(File Transfer Protocol，FTP)、电子邮件传输协议(Simple Mail Transfer Protocol，SMTP)、域名服务(Domain Name Service，DNS)、网上新闻传输协议(Net News Transfer Protocol，NNTP)和超文本传输协议(HyperText Transfer Protocol，HTTP)等。TELNET允许一台机器上的用户登录到远程机器上，并进行工作；FTP提供有效地将文件从一台机器上传输到另一台机器上的方法；SMTP用于电子邮件的收发；DNS用于把主机名映射到网络地址；NNTP用于新闻的发布、检索和获取；HTTP用于在WWW上获取主页。

1.3.2　OSI参考模型与TCP/IP参考模型的比较

1. 共同点

比较OSI模型与TCP/IP模型，这两个模型的共同点如下：

(1) 都采用了层次结构的概念。

(2) 都能够提供面向连接和无连接两种通信服务机制。

2. 不同点

比较OSI模型与TCP/IP模型，这两者也存在许多的不同点：

(1) OSI采用7层结构，而TCP/IP采用4层结构。

(2) TCP/IP 参考模型的网络接口层实际上并没有真正的定义，只是一些概念性的描述；OSI 参考模型不仅分了两层，而且对每一层的功能都很详尽地描述，甚至在数据链路层又分出一个介质访问子层，用于专门解决局域网的共享介质问题。

(3) OSI 模型是在协议开发前设计的，具有通用性；TCP/IP 是先有协议集，然后建立模型，不适用于非 TCP/IP 网络。

(4) OSI 参考模型与 TCP/IP 参考模型的传输层功能基本相似，都是负责为用户提供真正的端对端的通信服务，也对高层屏蔽了底层网络的实现细节。所不同的是，TCP/IP 参考模型的传输层是建立在网络互联层基础之上的，而网络互联层只提供无连接的网络服务，所以面向连接的功能完全在 TCP 中实现。当然，TCP/IP 的传输层还提供无连接的服务，如 UDP；相反，OSI 参考模型的传输层是建立在网络层基础之上的，网络层既提供面向连接的服务，又提供无连接的服务，但传输层只提供面向连接的服务。

(5) OSI 参考模型的抽象能力高，适合于描述各种网络；而 TCP/IP 是先有了协议，然后才制定 TCP/IP 模型。

(6) OSI 参考模型的概念划分清晰，但过于复杂；而 TCP/IP 参考模型在服务、接口和协议的区别上不清楚，功能描述和实现细节混在一起。

(7) TCP/IP 参考模型的网络接口层并不是真正的一层；OSI 参考模型的缺点是层次过多，划分意义不大，但增加了复杂性。

(8) OSI 参考模型虽然被看好，但是由于没把握好时机，技术不成熟，实现起来仍很困难；相反，虽然 TCP/IP 参考模型有许多不尽如人意的地方，但还是比较成功的。TCP/IP 才是事实上的国际通用的计算机网络标准。

1.4 IPv4

1.4.1 IPv4 地址的概念

在 Internet 上连接的所有计算机——从大型机到微型计算机，都是以独立的身份出现的，我们称它为主机。为了实现各主机间的通信，每台主机都必须有一个唯一的网络地址。就好像每个住宅都有唯一的门牌一样，才不至于在传输资料时出现混乱。

Internet 的网络地址是指连入 Internet 的计算机的地址编号。所以，在 Internet 中，网络地址唯一地标识一台计算机。

我们都知道，Internet 是由几千万台计算机相互连接而成的。而我们要确认网络上的每台计算机，靠的就是能唯一标识该计算机的网络地址，这个地址就叫作 IP 地址，即用 Internet 协议语言表示的地址。

在 Internet 里，IPv4 地址是一个 32 位的二进制地址，为了便于记忆，将它们分为 4 组，每组 8 位，由小数点分开，用 4 字节来表示，而且用点分开的每字节的数值范围是十进制数 0～255，如 202.116.0.1，这种书写方法叫作点分十进制数表示法。

1.4.2 IPv4 简介

IPv4 是 IP 的第 4 版，也是第一个被广泛使用，构成如今国际互联网技术的基石的协议。1981 年，Jon Postel 在 RFC791 中定义了 IP。IPv4 可以运行在各种各样的底层网络

上，如端对端的串行数据链路(PPP 和 SLIP)、卫星链路等。局域网中最常用的是以太网。

无论网络用户是使用智能手机上网，还是使用 PC(个人计算机)上网，他的手机或 PC 都会被分配一个 IP 地址，手机或 PC 使用这个 IP 地址与互联网上的其他网元通信。IP 地址现在有 IPv4 和 IPv6 两大类，目前使用的绝大多数的 IP 地址是 IPv4 地址。

IPv4 是 Internet Protocol Version 4 的缩写，表示 IP 的第 4 个版本。目前，国际互联网上绝大多数的通信数据都是以 IPv4 数据包的格式封装的。IPv4 在 IETF Publication RFC 791 中有详细的描述。

IPv4 地址通常用点分十进制数表示法书写，如 192.168.0.1，其中的数字都是十进制的数字，中间用实心圆点分隔。

一个 IPv4 地址可以分为网络地址和主机地址两部分，其中网络地址可以使用如下形式描述：192.168.0.0/16，斜线后的数字表示网络地址部分的长度是 16 位，对应 2 字节，即网络地址部分是 192.168.0.0。

为了便于对 IP 地址进行管理，根据 IPv4 地址的第一个字节的取值范围，IPv4 地址可以分为以下 5 类。

A 类：0～127。

B 类：128～191。

C 类：192～223。

D 类：224～239，组播地址。

E 类：240～254，保留为研究测试使用。

此外，IPv4 地址中有一些地址段有特殊用途，可用于家庭、办公室和企业的内部局域网等。有特殊用途的地址段见表 1-1。

表 1-1　有特殊用途的地址段

地址范围	功能描述
10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	私网 IPv4 地址，可用于家庭、办公室和企业的内部局域网。设计私网 IPv4 地址的初衷是缓解 IPv4 地址耗尽问题
169.254.0.0/16	Link-local，该地址只在某网段有意义，路由器是不会转发地址为 Link-local 的 IP 包的
127.0.0.0/8	Loopback，回送测试(Loopback test)所用
224.0.0.0/4	IP 组播地址
240.0.0.0/4	保留为研究测试使用
255.255.255.255	广播地址

1.4.3　IPv4 报文格式

IPv4 的报文格式如图 1-3 所示。IPv4 的报文包括版本、首部长度、服务类型、报文总长度、标识符、标志、分段偏移、生存时间、协议、首部校验和、源 IPv4 地址、目标 IPv4 地址、可选项、数据和填充字段。

<table>
<tr><td>版本
4位</td><td>首部长度
4位</td><td>服务类型
8位</td><td colspan="2">报文总长度
16位</td></tr>
<tr><td colspan="3">标识符
16位</td><td>标志
3位</td><td>分段偏移
13位</td></tr>
<tr><td colspan="2">生存时间
8位</td><td>协议
8位</td><td colspan="2">首部校验和
16位</td></tr>
<tr><td colspan="5">源IPv4地址
32位</td></tr>
<tr><td colspan="5">目标IPv4地址
32位</td></tr>
<tr><td colspan="5">可选项</td></tr>
<tr><td colspan="5">数据</td></tr>
<tr><td colspan="5">填充</td></tr>
</table>

图 1-3　IPv4 的报文格式

IPv4 报文各字段的功能说明如下：

版本(Version)字段：标识了数据包的 IP 版本号，占 4 位，取值为 0100 时，表示 IPv4；取值为 0110 时，表示 IPv6。

首部长度(IP Header Length，IHL)字段：表示数据包的报头部分的长度，占 4 位，指向数据的起点。正确报文头的最小值为 5。

服务类型(Type of Service，TOS)字段：用来指定特殊的数据包处理方式，占 8 位。

报文总长度(Total Length，TL)字段：接收方用 IP 数据包的总长度减去首部长度，就可以确定数据包数据有效载荷的大小。

标识符(Identification)字段：通常与标记字段和分片字段一起用于数据包的分段，长度为 16 位。

标志(Flags)字段：用于区分不同的 IP 数据包，长度只有 3 位。

分段偏移(Fragment Offset)字段：用于指明分段起始点相对于报头起始点的偏移量，可以使接收者按照正确的顺序重组数据包，长度为 13 位。

生存时间(Time to Live，TTL)字段：用于防止数据包在网络上无休止地被传输，长度为 8 位。

协议(Protocol)字段：指定了数据包中信息的类型，长度为 8 位。

首部校验和(Header Checksum)字段：是用于检测 IP 报头传输是否出现错误的字段，长度为 16 位，帮助确保 IP 头的完整性。由于某些协议头字段(如生存时间)的改变，就需要对每个点重新计算和检验。

源 IPv4 地址(Source IPv4 Address)字段：表示发送方数据包源点的 IP 地址，长度为 32 位。

目标 IPv6 地址(Destination IPv6 Address)字段：表示接收方的 IP 地址，长度为 32 位。

可选项(Options)字段：被添加在 IP 报头中，包括源点产生的信息和其他路由器加入的信息。可选项字段主要用于测试，长度可变。

数据(Data)字段：用于存放数据包的数据，长度可变。

填充(Padding)字段：通过在可选字段后面添加 0 来补足 32 位，以确保报头长度是 32 的倍数。

1.4.4　IPv4 的不足之处

IPv4 使用 32 位二进制位的地址，因此 IPv4 的地址空间是 $2^{32}=4\ 294\ 967\ 296$。最初每个连接入互联网的用户都被分配使用一个 IPv4 地址，因此未分配的 IPv4 地址越来越少，由此产生了 IPv4 地址耗尽的问题。为了从根本上解决 IPv4 地址耗尽的问题，IPv6 应运而生。

传统的 TCP/IP 基于 IPv4。它的最大问题是网络地址资源有限，从理论上讲，编址 1600 万个网络、40 亿台主机。但采用 A、B、C 三类编址方式后，可用的网络地址和主机地址的数目大打折扣，以至于 IP 地址已经枯竭。其中北美占有 3/4，约 30 亿个，而人口最多的亚洲只有不到 4 亿个，中国截至 2010 年 6 月，IPv4 地址数量达到 2.5 亿个，落后于 4.2 亿网民的需求。虽然用动态 IP 及 NAT 地址转换等技术实现了一些缓冲，但 IPv4 地址枯竭已经成为不争的事实。传统的 TCP/IP 基于电话宽带以及以太网的电器特性而制定，其分包原则与检验占用数据包很大的比例，造成传输效率低。目前，国际互联网正向着全光纤网络和高速以太网方向发展，TCP/IP 不能满足其发展需求。

因此，互联网工程任务组(Internet Engineering Task Force，IETF)专家提出 IPv6 的互联网技术正在推行，但从 IPv4 的使用过渡到 IPv6 需要很长的一段时间。中国目前主要使用的仍然是 IPv4。虽然在 Windows 7 系统中已经支持 IPv6 的协议，不过对于广大的网络用户来说，过渡到 IPv6 可能还需要很长一段时间。

1.5　IPv6

IPv6 是英文 Internet Protocol Version 6 的缩写，其中 Internet Protocol 译为“因特网协议”。IPv6 是 IETF 设计的用于替代当前仍然在使用的 IPv4 协议的下一代国际互联网协议。IPv6 号称可以为全世界的每一粒沙子分配一个独立的网络地址。

IPv4 最大的问题在于网络地址资源有限，这严重制约了互联网的应用和发展。IPv6 技术的应用，不仅能解决网络地址资源数量的问题，而且也跨越了多种接入设备连入互联网的障碍。

1.5.1　IPv6 地址的表示方法

IPv6 的地址长度为 128 位，是 IPv4 地址长度的 4 倍。在 IPv6 中，原来 IPv4 的点分十进制格式已经不再适用，IPv6 地址改用十六进制表示。IPv6 地址有 3 种表示方法。

1. 冒分十六进制表示法

格式为 X:X:X:X:X:X:X:X，其中每个 X 表示地址中的 16 位，以十六进制表示。例如：

ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

这种表示法中，每个X的前导0是可以省略的，例如：

2001:0EC8:0000:002A:000B:0800:200C:417A→2001:EC8:0:2A:B:800:200C:417A

2. 0位压缩表示法

在某些情况下，一个IPv6地址中间可能包含很长的一段0，可以把连续的一段0压缩为"::"。但是，为了保证地址解析的唯一性，地址中的省略符号"::"只能出现一次，例如：

FDA1:0:0:0:0:0:0:1101→FDA1::1101

0:0:0:0:0:0:0:D→::D

0:0:0:0:0:0:0:0→::

3. 内嵌IPv4地址表示法

为了实现IPv4与IPv6互通，IPv4地址会嵌入IPv6地址中，此时地址常表示为X:X:X:X:X:X:d.d.d.d，前96位采用冒分十六进制表示，而最后32位地址则使用IPv4的点分十进制表示。例如，::192.168.0.1与::FFFF:192.168.0.1就是两个典型的例子，注意在前96位中，压缩0位的方法仍然适用。

1.5.2 IPv6的地址类型

IPv6协议主要定义了3种地址类型：单播地址(Unicast Address)、组播地址(Multicast Address)和任播地址(Anycast Address)。与原来的IPv4地址相比，新增了"任播地址"类型，取消了原来IPv4地址中的广播地址，因为在IPv6中的广播功能是通过组播来完成的。

1. 单播地址

单播地址用来唯一标识一个接口，类似于IPv4中的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的一个接口。

2. 组播地址

组播地址用来标识一组接口(通常这组接口属于不同的结点)，类似于IPv4中的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。

3. 任播地址

任播地址用来标识一组接口(通常这组接口属于不同的结点)。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源结点最近(根据使用的路由协议进行度量)的一个接口。

IPv6地址类型由地址前缀部分确定，主要地址类型与地址前缀的对应关系见表1-2。

表1-2 IPv6地址类型与前缀的对应关系

地址类型		地址前缀(二进制)	IPv6前缀标识
单播地址	未指定地址	00…0(128位)	::/128
	环回地址	00…1(128位)	::1/128
	链路本地地址	1111111010	FE80::/10
	站点本地地址	1111111011	FEC0::/10
	全球单播地址	其他形式	—
组播地址		11111111	FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式	

1.5.3　IPv6 的核心协议

IPv6 的核心协议主要包括 Internet 协议版本（IPv6）、Internet 控制消息协议（ICMPv6）、组播侦听者发现协议（MLD）和邻居发现协议等。

1. Internet 协议版本

IPv6 协议是在 RFC 2460 Internet Protocol Version 6（IPv6）Specification 中定义的。IPv6 协议是一种无连接的、不可靠的数据报协议，主要用于在主机之间寻址和路由数据包。

无连接意味着交换数据之前没有建立会话，不可靠意味着传送没有保障。IPv6 总是尽力尝试传送数据包。IPv6 数据包有可能丢失、不按顺序传递、重复或延迟。IPv6 不尝试从这些错误类型中恢复。所传递的数据包的确认以及丢失数据包的恢复由更高层的协议（如 TCP）来完成。

IPv6 数据包也称为 IPv6 数据报。如上所述，IPv6 数据包由 IPv6 报头和 IPv6 有效载荷组成。

2. Internet 控制消息协议

ICMPv6（Internet Control Message Protocol Version 6），即互联网控制信息协议第 6 版。互联网控制信息协议是 IP 的一个重要组成部分。ICMPv6 是为了与 IPv6 配套使用而开发的互联网控制信息协议。与 IPv4 一样，IPv6 也需要使用 ICMP，旧版本的 ICMP 不能满足 IPv6 的全部要求，因此开发了新版本的 ICMP，称为 ICMPv6。

ICMPv6 向源结点报告关于目的地址传输 IPv6 包的错误和信息，具有差错报告、网络诊断、邻结点发现和多播实现等功能。在 IPv6 中，ICMPv6 实现 IPv4 中 ICMP、ARP 和 IGMP 的功能。国际互联网地址授权委员会（IANA）定义 ICMPv6 的协议号为 58。邻居发现（ND）协议是基于 ICMPv6 协议的。

ICMPv6 协议的基本功能包括以下 4 点：

（1）通告网络错误。例如，某台主机或整个网络由于某些故障不可达。如果有指向某个端口号的 TCP 或 UDP 包没有指明接收端，也由 ICMP 报告。

（2）通告网络拥塞。当路由器缓存太多包，由于传输速率无法达到它们的接收速率，将会生成“ICMP 源结束”信息。对于发送者，这些信息将会导致传输速率降低。当然，更多的 ICMP 源结束信息的生成也将引起更多的网络拥塞，所以使用起来较为保守。

（3）协助解决故障。ICMP 支持 Echo 功能，即在两个主机间一个往返路径上发送一个包。Ping 是一种基于这种特性的通用网络管理工具，它将传输一系列的包，测量平均往返次数并计算丢失百分比。

（4）通告超时。如果一个 IP 包的 TTL（生存时间值）降低到零，路由器就会丢弃此包，这时会生成一个 ICMP 包通告这一事实。

3. 组播侦听者发现协议

组播侦听者发现（Multicast Listener Discover，MLD）协议是组播技术中使用的一种网络协议。它用于 IPv6 路由器在其直连网段上发现组播侦听者。

组播侦听者发现协议与现在广泛使用的单播协议的不同之处在于发送次数大大减少。当有 n 个接收主机时，发送方主机用单播协议向这 n 个主机发送相同的数据时，发送主机需要分别逐一向这 n 个主机发送，共需要发送 n 次；而当这个主机用组播协议向 n 个主机发

送相同的数据时，只需要发送1次，其数据由网络中的路由器和交换机逐级进行复制并发送给各个接收方，这样既节省服务器资源，也节省网络主干的带宽资源。

与广播协议相比，只有组播接收方向路由器发出请求后，网络路由器才复制一份数据给接收方，从而节省接收方的带宽。而广播方式无论接收方是否需要，网络设备都将所有广播信息向所有设备发送，从而大量占据接收方的接入带宽。

组播侦听者（Multicast Listener）是那些希望接收组播数据的主机结点。

路由器通过MLD协议，可以了解自己的直连网段上是否有IPv6组播组的侦听者，并在数据库里做相应记录。同时，路由器还维护与这些IPv6组播地址相关的定时器信息。

MLD路由器使用IPv6单播链路本地地址作为源地址发送MLD报文。MLD使用ICMPv6（针对IPv6的互联网控制报文协议）报文类型。所有的MLD报文被限制在本地链路上，跳数为1。

4. 邻居发现协议

邻居发现（Neighbor Discovery，ND）协议是专门为IPv6开发的主动查找邻居的专用协议，由RFC2461定义，它可以使当前结点（主机和路由器）发现本链路上其他邻居的数据链路层地址。主机可以使用邻居发现协议发现邻近的路由器，把它作为自己的默认网关；结点使用邻居发现协议主动跟踪邻居是否可达，并检测邻居数据链路层地址的改变。当结点或到达邻居的路径失效时，主机依靠该协议主动搜索可用的路由器或路径。

概括起来，邻居发现协议解决的是在统一链路上的结点之间的交互问题，这些问题包括路由器发现、前缀发现、参数发现、IPv6地址自动配置、地址解析、下一跳确定、邻居不可达检测、重复地址检测、重定向等。

邻居发现协议使用以下5种类型的ICMPv6数据包工作：

(1) 路由器请求：当接口启动后，主机发送该信息请求路由器立即产生路由器宣告消息。

(2) 路由器宣告：路由器在定期接收到路由器请求信息后，使用该信息向链路上宣告它的存在，该数据包中携带有用来进行地址自动配置的前缀等信息。

(3) 邻居请求：结点使用该信息确定邻居的数据链路层地址，或缓存的邻居的数据链路层地址是否可达，该信息也用来进行重复地址检测。

(4) 邻居宣告：对邻居请求信息的回应信息，结点也可以发送未被请求的邻居宣告（Unsolicited Neighbor Advertisement）信息通告数据链路层地址的更改。

(5) 重定向：指当某一条路由出现故障时，自动在路由表中将此故障路由更新为另一条可用的路由，从而保证网络数据传输的畅通。

1.5.4 IPv6报文格式

IPv6报文的整体结构分为IPv6报头、扩展报头和上层协议数据3部分。IPv6报头是必选报文头部，长度固定为40B，包含该报文的基本信息；扩展报头是可选报头，可能存在0个、1个或多个，IPv6协议通过扩展报头实现各种丰富的功能；上层协议数据是该IPv6报文携带的上层数据，可能是ICMPv6报文、TCP报文、UDP报文或其他报文。

IPv6的报文格式如图1-4所示。IPv6的报文包括版本、流量等级、流标签、载荷长度、下一报头、跳数限制、源IPv6地址、目标IPv6地址和有效载荷等字段。

<table>
<tr><td>版本
4位</td><td>流量等级
8位</td><td colspan="2">流标签
24位</td></tr>
<tr><td colspan="2">载荷长度
16位</td><td>下一报头
8位</td><td>跳数限制
8位</td></tr>
<tr><td colspan="4">源IPv6地址
128位</td></tr>
<tr><td colspan="4">目标IPv6地址
128位</td></tr>
<tr><td colspan="4">有效载荷</td></tr>
</table>

图 1-4　IPv6 的报文格式

(1) 版本：表示协议版本，占 4 位，取值为 0110。

(2) 流量等级：占 8 位，主要用于 QoS。

(3) 流标签：占 24 位，用来标识同一个流里面的报文。

(4) 载荷长度：占 16 位，表明该 IPv6 包头部后包含的字节数，包含扩展头部。

(5) 下一报头：占 8 位，该字段用来指明报头后接的报文头部的类型，若存在扩展头，表示第一个扩展头的类型，否则表示其上层协议的类型，它是 IPv6 各种功能的核心实现方法。

(6) 跳数限制：占 8 位，该字段类似于 IPv4 中的生存时间，每次转发跳数减 1，当该字段达到 0 时，数据包将会被丢弃。

(7) 源 IPv6 地址：占 128 位，标识该报文的来源 IPv6 地址。

(8) 目标 IPv6 地址：占 128 位，标识该报文的目标 IPv6 地址。

(9) 有效载荷：有效载荷由 IPv6 报头、路由扩展头、分片扩展头、TCP 头和 TCP 数据等部分组成，如图 1-5 所示。

IPv6报头 下一报头=TCP	TCP头+TCP数据

(a) 0个扩展头

IPv6报头 下一报头=路由头	路由扩展头 下一报头=TCP	TCP头部+TCP数据

(b) 1个扩展头

IPv6报头 下一报头=路由头	路由扩展头 下一报头=分片	分片扩展头 下一报头=TCP	TCP头+TCP数据

(c) 2个扩展头

图 1-5　IPv6 扩展头的使用示例

IPv6 报文中不再有“选项”字段，而是通过“下一报头”字段配合 IPv6 扩展报头来实现选项的功能。使用扩展头部时，将在 IPv6 报文下一报头字段表明首个扩展报头的类型，再根据该类型对扩展报头进行读取与处理。每个扩展报头同样包含下一报头字段，若接下来

有其他扩展报头，即在该字段中继续标明接下来的扩展报头的类型，从而达到添加连续多个扩展报头的目的。在最后一个扩展报头的下一报头字段中，则标明该报文上层协议的类型，用以读取上层协议数据。

1.6 本章总结

网络互联是指将两个以上的通信网络通过一定的技术与方法，用一种或多种网络通信设备相互连接起来，以构成更大的网络系统。网络互联的目的是实现不同网络中的用户可以互相通信、共享软件和数据等。

为进行计算机网络中的数据交换而建立的规则、标准或约定称为网络协议（network protocol）。网络协议简称为协议。准确地说，网络协议主要由以下 3 个要素组成：

（1）语法：即数据与控制信息的结构或格式。

（2）语义：即需要发出何种控制信息，完成何种动作和做出何种响应。

（3）同步：即事件实现顺序的详细说明。

在网络体系结构中，用分层来实现网络的结构化设计。网络分层就是将网络结点中的数据发送或转发、打包或拆包，控制信息的加载或拆出等工作，分别由不同的硬件和软件模块去完成。这样，可以使往来通信和网络互联这一复杂的问题变得较为简单。

分层时应注意使每层的功能明确。分层的层数不能太少，也不能太多。因为层数太少，会使每一层的协议太复杂；层数太多，又会在描述和综合各层功能的系统工程任务时遇到较多的困难。

OSI 参考模型是国际标准化组织在 1984 年提出的网络互联模型。该体系结构标准定义了网络互联的七层框架，即物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

TCP/IP 参考模型是首先由 ARPANET 使用的网络体系结构。这个体系结构在它的两个主要协议出现以后被称为 TCP/IP 参考模型（TCP/IP Reference Model）。TCP/IP 参考模型自下而上共分为 4 层：网络接口层、互联网层、传输层和应用层。

在 Internet 里，IPv4 地址是一个 32 位的二进制地址，为了便于记忆，将它们分为 4 组，每组 8 位，由小数点分开，用 4 个字节表示，而且用点分开的每个字节的数值范围是十进制数 0～255，如 202.116.0.1，这种书写方法叫作点分十进制数表示法。

一个 IPv4 地址可以分为网络地址和主机地址两部分，其中网络地址可以使用如下形式描述：192.168.0.0/16，斜线后的数字表示网络地址部分的长度是 16 位，对应 2 个字节，即网络地址部分是 192.168.0.0。

为了便于对 IP 地址进行管理，根据 IPv4 地址的第一个字节，IPv4 地址可以分为 5 类。

IPv4 的报文包括版本、首部长度、服务类型、报文总长度、标识符、标志、分段偏移、生存时间、协议、首部校验和、源 IPv4 地址、目标 IPv4 地址、可选项、数据和填充字段。

IPv4 使用 32 位二进制位的地址，因此 IPv4 的地址空间是 $2^{32}=4\ 294\ 967\ 296$。最初每个接入互联网的用户都被分配使用一个 IPv4 地址，因此未分配的 IPv4 地址越来越少，由此产生了 IPv4 地址耗尽的问题。为了从根本上解决 IPv4 地址耗尽的问题，IPv6 应运而生。

IPv6 的地址长度为 128 位，是 IPv4 地址长度的 4 倍。在 IPv6 中，原来 IPv4 的点分十进制格式已经不再适用，IPv6 地址改用十六进制表示。IPv6 地址有 3 种表示方法，即冒分十六进制表示法、0 位压缩表示法和内嵌 IPv4 地址表示法。

IPv6 协议主要定义了 3 种地址类型：单播地址(Unicast Address)、组播地址(Multicast Address)和任播地址(Anycast Address)。与原来在 IPv4 地址相比，新增了“任播地址”类型，取消了原来 IPv4 地址中的广播地址，因为在 IPv6 中的广播功能是通过组播来完成的。

IPv6 的核心协议主要包括 Internet 协议版本(IPv6)、Internet 控制消息协议(ICMPv6)、组播侦听者发现协议(MLD)和邻居发现协议等。

IPv6 报文的整体结构分为 IPv6 报头、扩展报头和上层协议数据 3 部分。

复习思考题

1. 什么是网络协议？
2. 网络协议的 3 个要素是什么？
3. 为什么计算机网络要划分层次？
4. OSI 参考模型把计算机网络分为哪几层？每一层的主要功能是什么？
5. TCP/IP 参考模型把计算机网络分为哪几层？每一层的主要功能是什么？
6. 请比较 OSI 参考模型与 TCP/IP 参考模型有什么异同点。
7. IPv4 地址占几位二进制数？IPv4 地址分为哪几类？各类的地址范围是什么？
8. 请用表格说明有特殊用途的 IPv4 的地址段。
9. 请画图说明 IPv4 的报文格式。
10. 什么是 IPv6 协议？
11. IPv6 地址可以用哪些方法表示？
12. IPv6 地址可以分为哪些类型？
13. IPv6 的核心协议主要包括哪些协议？
14. 请画图说明 IPv6 的报文格式。

第 2 章 网络互联设备

CHAPTER 2

在第 1 章学习网络参考模型的基础上，我们将在本章逐一讨论网络互联涉及的各种传输介质和设备，包括各种有线和无线传输介质、物理层设备、数据链路层设备、网络层设备、应用层设备等。

2.1 网络传输介质

网络传输介质是指在网络中传输信息的载体。常用的传输介质分为有线传输介质和无线传输介质两大类。

有线传输介质是指在两个通信设备之间实现的物理连接部分，它能将信号从一端传输到另一端，有线传输介质主要有双绞线、同轴电缆和光纤。双绞线和同轴电缆传输电信号，光纤传输光信号。

无线传输介质指我们周围的自由空间。我们利用无线电波在自由空间的传播可以实现多种无线通信。在自由空间传输的电磁波根据频谱可分为无线电波、微波、红外线和激光等，信息被加载在电磁波上进行传输。

不同的传输介质，其特性也各不相同。它们不同的特性对网络中的数据通信质量和通信速度有较大影响。

2.1.1 连接器

连接器是连接电缆与网络设备的硬件。网络设备可以是一个文件服务器、工作站、交换机或打印机。每种网络介质都对应一种特定类型的连接器。所使用的连接器的种类将影响网络安装和维护的成本、网络增加段和结点的容易度。例如，常用的双绞线要用 RJ-45 连接器来连接。RJ-45 连接器如图 2-1 所示。又如，用于 UTP 电缆的连接器（看上去更像一个大的电话线连接器）在接入和替换时，比用于同轴电缆的连接器的插入和替换要简单得多。UTP 电缆连接器更廉价，并可用于许多不同的介质和设备。

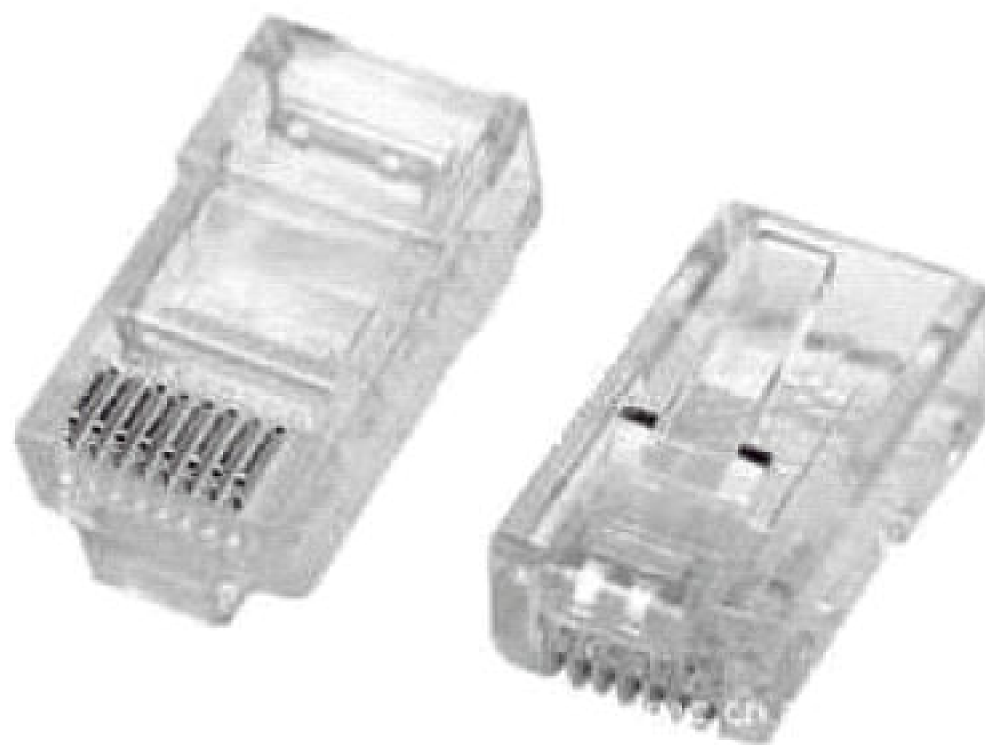


图 2-1 RJ-45 连接器

2.1.2 双绞线

双绞线简称TP,可将一对以上的双绞线封装在一个绝缘外套中,为了降低信号的干扰程度,电缆中的每对双绞线一般由两根绝缘铜导线相互扭绕而成,因此把它称为双绞线。双绞线可以分为非屏蔽双绞线(Unshielded Twisted Pair,UTP)和屏蔽双绞线(Shielded Twisted Pair,STP)两大类。非屏蔽双绞线和屏蔽双绞线的外形如图2-2所示。

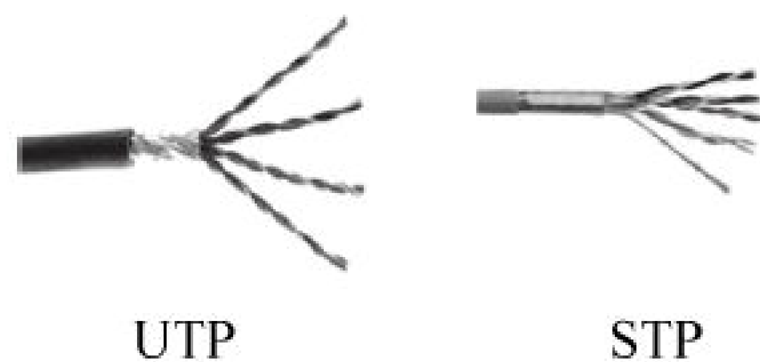


图2-2 非屏蔽双绞线和屏蔽双绞线的外形

非屏蔽双绞线的价格比较便宜,但传输速率偏低,抗干扰能力较差,适合于短距离通信;屏蔽双绞线抗干扰能力较好,具有更高的传输速率,但价格相对较高。

双绞线需用RJ-45或RJ-11连接头插接。

目前市场上销售的非屏蔽双绞线可以分为4种:3类双绞线、4类双绞线、5类双绞线和超5类双绞线。

1. 3类双绞线

3类双绞线的传输速率支持10Mb/s,外层保护胶皮较薄,皮上注有"cat3"字样。

2. 4类双绞线

4类双绞线的传输速率支持10Mb/s,在网络中不常用。

3. 5类双绞线

5类双绞线的传输速率支持100Mb/s或10Mb/s,外层保护胶皮较厚,皮上注有"cat5"字样。

4. 超5类双绞线

超5类双绞线在传送信号时比普通5类双绞线的衰减更小,抗干扰能力更强,在100M网络中,受干扰程度只有普通5类线的1/4,这类双绞线的应用较少。

屏蔽双绞线(STP)也分为3类和5类两种。STP的内部结构与UTP相同,外面包着铝箔,起屏蔽作用,所以抗干扰能力强、传输速率高,但价格较贵。

星形以太网采用双绞线连接,双绞线是8芯,分4组,两芯一组绞在一起,故称双绞线。

8芯双绞线虽然共有8根线,但是实际上只用了其中4根线:1、2、3、6。

常见的接线方式有两种:568B接线规范(表2-1)和568A接线规范(表2-2)。

表2-1 568B接线规范

白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
1	2	3	4	5	6	7	8

表2-2 568A接线规范

白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
3	6	1	4	5	2	7	8

将568B接线规范的1和3对调,2和6对调,就可以得到568A接线规范。

如果双绞线的两端都使用568B接线规范,则称为直通线;如果双绞线一端使用568B

接线规范,而另一端使用 568A 规范,则称为交叉线。

双绞线一般用于星形网的布线连接,两端安装有 RJ-45 头(水晶头)、连接网卡与集线器,最大网线长度为 100m,如果要加大网络的范围,在两段双绞线之间可安装中继器,最多可安装 4 个中继器,如安装 4 个中继器连 5 个网段,最大传输范围可达 500m。

2.1.3 同轴电缆

同轴电缆具有抗干扰能力强、连接简单等特点,信息传输速率可达每秒几百兆位,是中、高档局域网的首选传输介质。



图 2-3 同轴电缆的内部结构

同轴电缆的内部结构如图 2-3 所示,由一根空心的外圆柱导体和一根位于中心轴线的内导线组成,内导线和圆柱导体及外界之间用绝缘材料隔开。同轴电缆需用带 BNC 头的 T 型连接器连接。

按同轴电缆的直径区分,可以分为粗缆和细缆两种。

1. 粗缆

粗缆的直径为 10mm,传输距离较长,性能较好,但是成本高,网络安装、维护困难,一般仅用于大型局域网的干线,连接时两端需要安装 100Ω 的终结电阻。

(1) 粗缆与外部收发器相连。

(2) 收发器与网卡之间用 AUI 电缆相连。

(3) 网卡必须有 AUI 接口(15 针 D 型接口):每段 500m,最多 100 个用户,4 个中继器可达 2500m,收发器之间的电缆长度最小 2.5m,最大 50m。

2. 细缆

细缆的直径为 5mm,连接时两端需要安装 50Ω 的终结电阻。与 BNC(基本网络卡)相连时用 T 型连接头,T 型头之间的距离最小应为 0.5m。细缆网络每段干线长度最大为 185m,每段干线最多接入 30 个用户。如采用 4 个中继器连接 5 个网段,网络最大距离可达 925m。

细缆安装较容易,造价较低,但日常维护不方便,一旦一个用户出故障,便会影响其他用户的正常工作。

2.1.4 光纤

光纤的外形如图 2-4 所示。

光纤又称为光缆或光导纤维,由光导纤维纤芯、玻璃网层和能吸收光线的外壳组成。

光纤是由一组光导纤维组成的用来传播光束的、直径细小而柔韧的传输介质。应用光学原理,由光发送机产生光束,将电信号调制为光信号,再把光信号导入光纤,在另一端由光接收机接收光纤上传来的光信号,并把它解调为电信号,经解码后再处理。

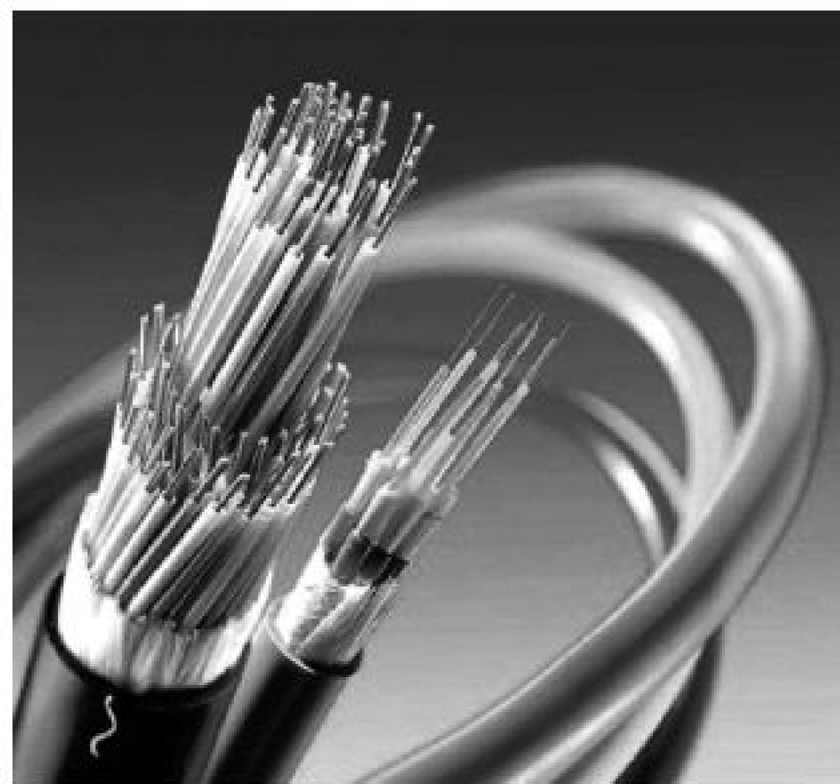


图 2-4 光纤的外形

光纤可以分为单模光纤和多模光纤。

1. 单模光纤

单模光纤由激光器作为光源，仅有一条光通路，传输距离较长，一般为20～120km。

2. 多模光纤

多模光纤由二极管作为光源，可以同时传输多束不同波长的光线，但是传输速率较低，传输距离较短，一般都少于2km。

光纤需用ST型连接器连接。

与其他传输介质相比，光纤具有电磁绝缘性能好、信号衰减极小、频带宽、传输速率高、传输距离远等特点，主要用于要求传输距离较长、布线条件特殊的主干网连接，具有不受外界电磁场的影响、无限制的带宽等优势，可以实现每秒万兆位的数据传送，尺寸小、重量轻，数据可传送几百千米，但价格昂贵。

2.1.5　无线传输介质

常用的无线传输介质有微波、红外线和无线电波。

1. 微波

微波是指频率为300MHz～300GHz的电磁波，是无线电波中一个有限频带的简称，即波长在1m(不含1m)到1mm之间的电磁波，是分米波、厘米波、毫米波的统称。微波频率比一般的无线电波频率高，通常也称为“超高频电磁波”。

微波的特点是：

(1) 只能进行可视范围内的通信。

(2) 大气对微波信号的吸收与散射影响较大。

(3) 微波通信主要用于几千米范围内，不适合铺设有线传输介质的情况，而且只能用于点到点的通信，传输速率也不高，一般为几百Kbps。

2. 红外线

红外线是太阳光线中众多不可见光线中的一种，由德国科学家霍胥尔(huoxuer)于1800年发现，又称为红外热辐射，他将太阳光用三棱镜分解开，在各种不同颜色的色带位置上放置了温度计，试图测量各种颜色的光的加热效应。结果发现，位于红光外侧的那支温度计升温最快。因此得到结论：太阳光谱中，红光的外侧必定存在看不见的光线，这就是红外线。红外线也可以用作传输的介质。太阳光谱上红外线的波长大于可见光线，波长为0.75～15.0μm。红外线可分为3类，即近红外线，波长在0.75～1.50μm之间；中红外线，波长在1.50～6.0μm之间；远红外线，波长在6.0～15.0μm之间。

红外线具有容量大，保密性强，抗电磁干扰性能好，设备结构简单、体积小、重量轻、价格低，但在大气信道中传输时易受气候影响的特点。大气对红外线辐射传输的影响主要是吸收和散射。

在不能架设有线线路，而使用无线电通信方式又怕泄密的情况下，使用红外线通信是比较好的选择。

3. 无线电波

无线电波是指在自由空间(包括空气和真空)传播的射频频段的电磁波。无线电技术是通过无线电波传播声音或其他信号的技术。

无线电技术的原理在于，导体中电流强弱的改变会产生无线电波。利用这一现象，通过

调制可将信号加载于无线电波之上。当电波通过空间传播到接收端，电波引起的电磁场变化又会在接收天线中感生交变电流。通过解调将信号从交变电流中提取出来，就达到了信息传输的目的。

2.2 物理层设备

一般来说，物理层是指 OSI 参考模型中的最低层。常用的物理层设备有中继器(Repeater，RP)、集线器(HUB)和无线接入点(Access Point，AP)等。工作在物理层的设备由于性能的限制，无法分辨出传输信号中的数据信息，其任务就是为与它互相连接的设备提供一个传输数据的物理连接。数据流在物理信道上以信号的方式进行传输。物理层设备确保原始的比特数据流在物理信道上有效传输。

2.2.1 中继器

中继器(Repeater，RP)是工作在物理层上的连接设备，适用于完全相同的两类网络的互联，主要功能是通过对数据信号的重新发送或者转发，来延长网络传输的距离。中继器是对信号进行再生和还原的网络设备，即是工作在 OSI 参考模型中物理层的设备。

中继器是局域网环境下用来延长网络距离的最简单、最廉价的网络互联设备。中继器对线路上的信号具有放大再生的功能，用于扩展局域网网段的长度(仅用于连接相同的局域网网段)。中继器的外形如图 2-5 所示。



图 2-5 中继器的外形

中继器是连接网络线路的一种装置，常用于两个网络结点之间物理信号的双向转发工作。中继器主要完成物理层的功能，负责在两个结点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的传输距离。由于存在损耗，在线路上传输的信号功率会逐渐衰减，衰减到一定程度时将造成信号失真，因此会导致网络传输故障。中继器就是为解决这一问题而设计的。它完成物理线路的连接，对衰减的信号进行放大，保持与原数据相同。一般情况下，中继器的两端连接的是相同的媒体，但有的中继器也可以完成不同媒体的转接工作。从理论上讲，中继器的使用是无限的，网络也因此可以无限延长。事实上，这是不可能的，因为网络标准中都对信号的延迟范围作了具体的规定，中继器只能在此规定范围内进行有效的工作，否则会引起网络故障。

2.2.2 集线器

集线器的英文为 Hub。Hub 是“中心”的意思。集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有结点集中在以它为中心的结点上。它也工作于 OSI 参考模型的最低层，即物理层。集线器与网卡、网线等传输介质一样，属于局域网中的基础设备，采用 CSMA/CD(带冲突检测的载波监听多路访问技术)介质访问控制机制。集线器的每个接口简单地收发比特，收到 1 就转发 1，收到 0 就转发 0，不进行碰撞检测。集线器的外形如图 2-6 所示。

集线器属于纯硬件网络底层设备，基本上不具有类似于交换机的“智能记忆”能力和“学习”能力。它也不具备交换机具有的 MAC 地址表，所以它转发数据时不是一对一的，而是采用广播方式发送。也就是说，当它要向某结点发送数据时，不是直接把数据发送到目的结点，而是把数据包发送到与集线器相连的所有结点。



图 2-6　集线器的外形

集线器是一个多端口的转发器，当以集线器为中心设备时，网络中某条线路产生了故障，并不影响其他线路的工作。所以，集线器在局域网中得到了广泛的应用。大多数的时候，它用在星形与树形网络拓扑结构中，以 RJ-45 接口与各主机相连。

集线器工作于 OSI 参考模型的物理层和数据链路层的 MAC(介质访问控制)子层。物理层定义了电气信号、符号、线的状态和时钟要求、数据编码和数据传输用的连接器。因为集线器只对信号进行整形、放大后再重发，不进行编码，所以是物理层的设备。10M 集线器在物理层有 4 个标准接口可用，那就是 10Base-5、10Base-2、10Base-T、10Base-F。10M 集线器的 AUI 端口用来实现总线网与以太网之间的连接。

集线器采用了 CSMA/CD(载波帧听多路访问/冲突检测)协议，CSMA/CD 为 MAC 层协议，所以集线器也含有数据链路层的功能。

集线器的工作过程非常简单，可以描述为：首先是结点发信号到线路，集线器接收该信号，因信号在电缆传输中有衰减，集线器接收信号后将衰减的信号整形放大，最后集线器将放大的信号广播转发给其他所有端口。

按结构和功能分类，集线器可分为未管理的集线器、堆叠式集线器和底盘集线器 3 类。

1. 未管理的集线器

最简单的集线器通过以太网总线提供中央网络连接，以星形的形式连接起来，通常称之为未管理的集线器，只用于很小型的(至多 12 个结点)网络中(在少数情况下，可以更多一些)。未管理的集线器没有管理软件或协议来提供网络管理功能，这种集线器可以是无源的，也可以是有源的。有源集线器使用得更多。

2. 堆叠式集线器

堆叠式集线器是稍微复杂一些的集线器。堆叠式集线器最显著的特征是多个集线器可以直接彼此相连，如图 2-7 所示。这样，只简单地添加集线器并将其连接到已经安装的集线器上，就可以扩展网络，这种方法不仅成本低，而且简单易行。

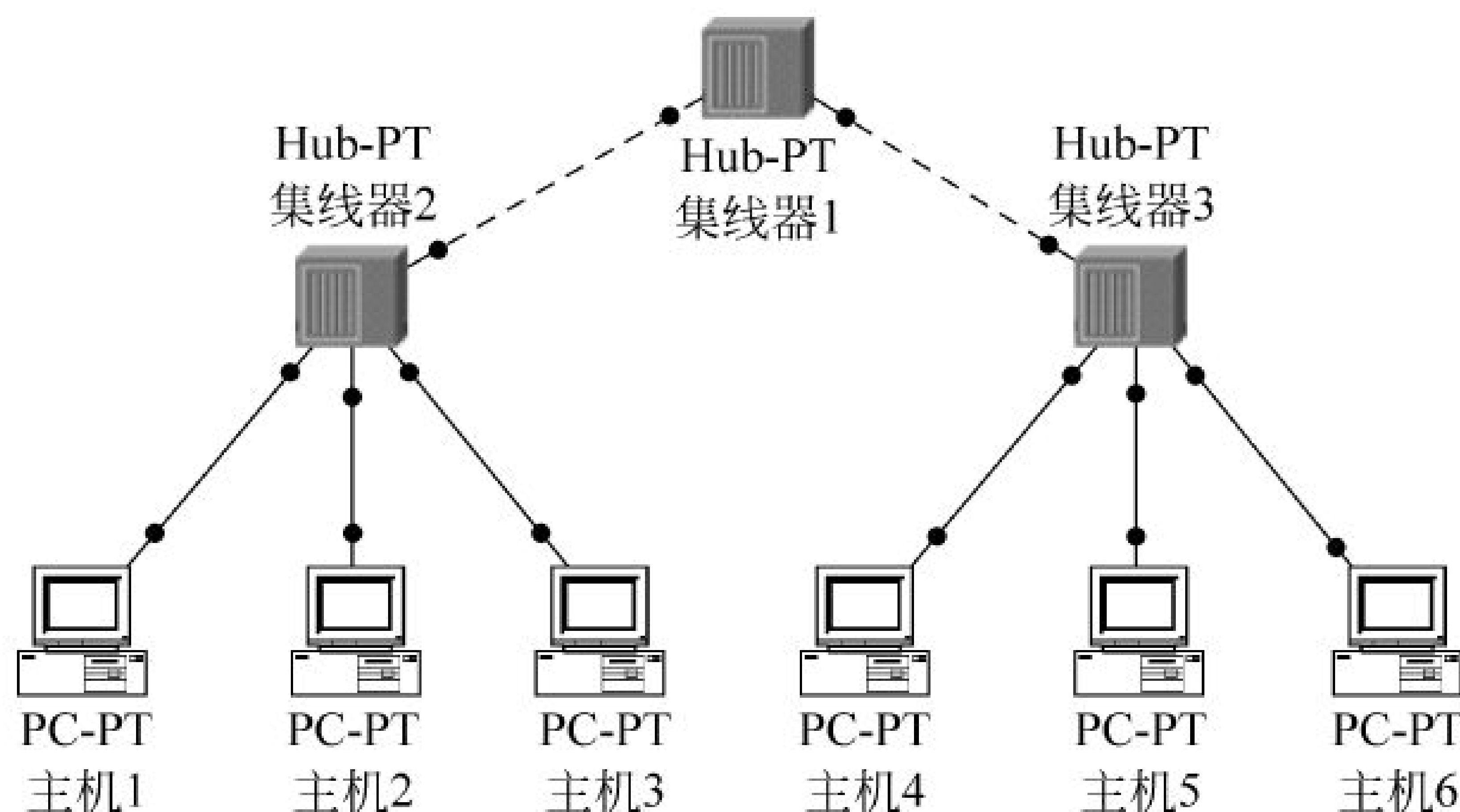


图 2-7　堆叠式集线器的工作原理

3. 底盘集线器

底盘集线器是一种模块化的设备,在其底板电路板上可以插入多种类型的模块。有些集线器带有冗余的底板和电源。同时,有些模块允许用户不必关闭整个集线器,便可替换那些失效的模块。集线器的底板给插入模块准备了多条总线,这些插入模块可以适应不同的网段,如以太网、快速以太网、光纤分布式数据接口(Fiber Distributed Data Interface,FDDI)和异步传输模式(Asynchronous Transfer Mode,ATM)中。有些集线器还包含有网桥、路由器或交换模块。有源的底盘集线器还可能会有重定时的模块,用来与放大的数据信号关联。

2.2.3 无线接入点

无线接入点(Access Point,AP)的外形如图 2-8 所示。

无线接入点是一个无线网络的接入点,俗称 WiFi“热点”,主要有路由交换接入一体设备和纯接入点设备。一体设备执行接入和路由工作,纯接入设备只负责无线客户端的接入。纯接入设备通常作为无线网络扩展使用,与其他 AP 或者主 AP 连接,以扩大无线覆盖范围,而一体设备一般是无线网络的核心。



图 2-8 无线接入点的外形

无线 AP 是使用无线设备(如手机等移动设备及笔记本电脑等无线设备)进入有线网络的接入点,主要用于宽带家庭、大楼内部、校园内部、园区内部以及仓库、工厂等需要无线监控的地方,典型距离覆盖几十米至上百米,也有可以用于远距离传送,目前最远的可以达到 30km 左右,主要技术为 IEEE 802.11 系列。大多数无线 AP 还带有接入点客户端模式(AP client),可以和其他 AP 进行无线连接,扩展网络的覆盖范围。

无线接入点的作用有两个:

(1) 作为无线局域网的中心点,供其他装有无线网卡的计算机通过它接入该无线局域网。

(2) 为有线局域网提供长距离的无线连接,或为小型无线局域网络提供长距离的有线连接,从而达到延伸网络范围的目的。

无线接入点也可以与小型无线局域网进行连接,从而达到拓展的目的。当无线网络用户足够多时,应当在有线网络中接入一个无线 AP,从而将无线网络连接至有线网络主干。AP 在无线工作站和有线主干之间起网桥的作用,实现了无线与有线的无缝集成。AP 既允许无线工作站访问网络资源,同时又为有线网络增加了可用资源。

无线 AP 接入点支持 2.4GHz 频段的无线应用,符合 802.11n 标准,并采用双路射频输出,每一路最大输出 600mW,可通过无线分布系统(点对点和点对多点桥接)在大面积的区域部署无线覆盖,是家庭和小型企业发展无线网络必备的无线 AP 设备。

一个典型的企业应用,就是在有线网络上安装数个无线接入点,实现企业内部网络的无线通信在无线接入点的接收范围内,无线用户端既有移动性的好处,又能充分与网络连接。在这种场合,无线接入点成为使用者接入有线网络的一个接口。另外一个用途则是

不允许使用有线电缆连接的情况。例如，制造商使用无线网络连接办公室和货仓之间的网络连线。

2.3　数据链路层设备

数据链路层是OSI参考模型中的第二层，介于物理层和网络层之间。数据链路层在物理层提供的服务的基础上向网络层提供服务，其最基本的服务是将源自网络层的数据可靠地传输到相邻结点的目标机网络层。为达到这一目的，数据链路必须具备一系列相应的功能，主要有：如何将数据组合成数据块，在数据链路层中称这种数据块为帧（帧是数据链路层传送的基本单位）；如何控制帧在物理信道上的传输，包括如何处理传输差错，如何调节发送速率，以使其与接收方相匹配；以及在两个网络实体之间提供数据链路通路的建立、维持和释放的管理。

数据链路可以理解为数据传输的通道。数据链路层位于物理层与网络层之间，是数据传输过程中比较重要的一层。物理层设备为终端设备提供传输媒介及连接，传输媒介是长期存在的，但通信设备之间的传输连接仅仅在通信时暂时连接。每次通信都要经过建立通信连接和拆除通信连接两个过程，这种建立起来的数据传输线路就称为数据链路。承担这种工作任务的设备就称为数据链路层设备。常用的数据链路层设备有网卡、网桥、交换机等。

2.3.1　网卡

网卡也称为网络适配器，是工作在数据链路层的网络组件。它是局域网中连接计算机和传输介质的接口，不仅能实现与局域网传输介质之间的物理连接和电信号匹配，还涉及帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据缓存的功能等。网卡的外形如图2-9所示。

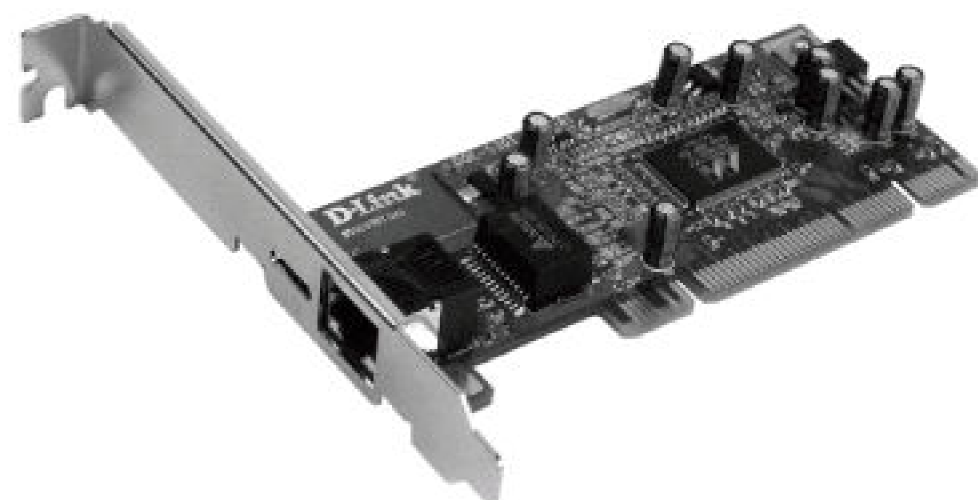


图2-9　网卡的外形

1. 网卡的工作原理

网卡可以分为有线网卡和无线网卡。这里，我们首先介绍有线网卡。

有线网卡上面装有处理器和存储器（包括RAM和ROM）。网卡和局域网之间的通信是通过电缆或双绞线以串行传输方式进行的。而网卡和计算机之间的通信则是通过计算机主板上的I/O总线以并行传输方式进行的。因此，网卡的一个重要功能就是要进行串行/并行转换。由于网络上的数据率和计算机总线上的数据率并不相同，因此在网卡中必须装有对数据进行缓存的存储芯片。

安装网卡时，必须将管理网卡的设备驱动程序安装在计算机的操作系统中。驱动程序是指挥网卡执行数据传输和存储的程序，决定应当从存储器的什么位置上将局域网传送过来的数据块存储下来。网卡还要能够实现以太网协议。

网卡并不是独立的自治单元，因为网卡本身不带电源，而是必须使用所插入的计算机的电源，并受该计算机的控制。因此，网卡可看作是一个半自治的单元。当网卡收到一个有差错的帧时，它会将这个帧丢弃，而不必通知它所插入的计算机。当网卡收到一个正确的帧

时，它就使用中断来通知该计算机并交付给协议栈中的网络层。当计算机要发送一个 IP 数据包时，它就由协议栈向下交给网卡组装成帧后发送到局域网。

随着集成度的不断提高，网卡上芯片的个数不断减少，虽然各个厂家生产的网卡种类繁多，但其功能大同小异。

2. 网卡的基本功能

1）数据的封装与解封

发送时将上一层（网络层）提供的数据包加上首部和尾部，封装成为以太网的帧。接收时则删除以太网帧的首部和尾部，然后送交上一层（网络层）。

2）链路管理

主要是实现 CSMA/CD（Carrier Sense Multiple Access with Collision Detection，带有冲突检测的载波监听多路访问）协议。

3）编码与译码

即曼彻斯特编码与译码。

3. 网卡的分类

针对不同的标准，网卡有不同的分类。

1）按网卡所属的主机类型分类

按网卡所属的主机类型分类，网卡一般分为工作站网卡和服务器专用网卡。

工作站网卡即我们常见的微机用的网卡，种类繁多，性能也有差异；而服务器专用网卡是专门针对网络服务器设计的，价格较贵，但性能很好。

2）按照网卡支持的带宽分类

按照网卡支持的带宽分类，可以分为 10M 网卡、100M 网卡、10/100M 自适应网卡、1000M 网卡 4 种。

3）按网卡总线的类型分类

按网卡总线的类型分类，可以把网卡分为 ISA 网卡、EISA 网卡和 PCI 网卡，其中，ISA 网卡和 PCI 网卡使用较多。ISA 总线网卡的带宽一般为 10M，PCI 总线网卡的带宽从 10M 到 1000M 都有。同样是 10M 网卡，因为 ISA 总线为 16 位，而 PCI 总线为 32 位，所以 PCI 网卡要比 ISA 网卡快。

4）按网卡的接口类型分类

按网卡的接口类型分类，可以把网卡分为 AUI 接口（粗缆接口）网卡、BNC 接口（细缆接口）网卡和 RJ-45 接口（双绞线接口）网卡 3 种类型。所以，在选用网卡时，应注意网卡支持的接口类型，否则可能不适用于你的网络。

市场上常见的 100M 网卡主要是 RJ-45 接口，带有 AUI 粗缆接口的网卡较少。除网卡的接口外，我们在选用网卡时还要注意网卡是否支持无盘启动（用于无盘工作站）。必要时还要考虑网卡是否支持光纤连接。

4. 无线网卡

无线网卡一般用于无线局域网中。无线局域网（Wireless Local Area Network，WLAN）就是利用无线电波作为信息传输的媒介构成的无线网络，与有线网络的用途十分类似，两者最大的不同在于传输媒介的不同，即利用无线电技术替代网线。

无线网卡是无线网络的终端设备，即在无线电波覆盖的环境下通过无线网络连接的终

端设备。具体来说，无线网卡就是使计算机可以利用无线电波来上网的一个设备，但是除了无线网卡，还需要一个可以提供无线网络连接服务的中央设备，即无线接入点（Access Point，AP）。无线接入点也称为无线路由器。如果安装了无线接入点，就可以通过无线网卡以无线的方式上网了。

无线网卡的工作原理是无线通信技术，计算机可以通过 WiFi、GPRS、CDMA、3G 和 4G 等几种无线数据传输模式来上网，除 WiFi 外，其余模式由中国移动、中国联通或中国电信实现。

大多数中小型企业和家庭主要是通过自己安装无线接入点建立 WiFi 基站来实现无线上网的。无线上网遵循 IEEE 802.11 系列（802.11b、802.11a、802.11d、802.11n 等）标准，通过无线传输，在无线接入点与无线网卡之间建立无线信道，实现数据的发送和接收。

按照 IEEE 802.11 协议，无线局域网卡分为媒体访问控制（MAC）层和物理层（PHY Layer）。在两者之间，还定义了一个媒体访问控制-物理（MAC-PHY）子层（Sublayers）。MAC 层提供主机与物理层之间的接口，并管理外部存储器，它与无线网卡硬件的 NIC（网络接口卡）单元对应。

物理层具体实现无线电信号的接收与发射，它与无线网卡硬件中的扩频通信机相对应。物理层提供空闲信道评估（Clear Channel Assessment，CCA）信息给 MAC 层，以便决定是否可以发送信号，通过 MAC 层的控制来实现无线网络的 CSMA/CA 协议，而 MAC-PHY 子层主要实现数据的打包与拆包，把必要的控制信息放在数据包的前面。

IEEE 802.11 协议指出，物理层必须有至少一种提供空闲信道估计 CCA 信号的方法。无线网卡的工作原理如下：当物理层接收到信号并确认无错后提交给 MAC-PHY 子层，经过拆包后把数据上交 MAC 层，然后判断是否是发给本网卡的数据，若是，则上交，否则丢弃。

如果物理层接收到的发给本网卡的信号有错，则需要通知发送端重发此包信息。当网卡有数据需要发送时，首先要判断信道是否空闲。若空闲，随机退避一段时间后发送；否则，暂不发送。由于网卡采用时分双工工作方式，所以，发送时不能接收，接收时不能发送。

常用的无线局域网络标准如下：

（1）IEEE 802.11b：使用 2.4GHz 频段，传输速度为 11Mb/s。

（2）IEEE 802.11a：使用 5GHz 频段，传输速度为 54Mb/s，与 802.11b 不兼容。

（3）IEEE 802.11g：使用 2.4GHz 频段，传输速度为 54Mb/s，可向下兼容 802.11b。

（4）IEEE 802.11n(Draft 2.0)：用于 Intel 新的迅驰 2 笔记本和高端路由上，可向下兼容，传输速度为 300Mb/s。

1997 年，电气与电子工程师学会（The Institute of Electrical and Electronics Engineers，IEEE）提出并制定了最早的无线标准 IEEE 802.11；在 1999 年 9 月又提出了 IEEE 802.11a 标准和 IEEE 802.11b 标准。

IEEE 802.11a、IEEE 802.11b 标准的出台以及 WiFi 组织的成立促进了无线局域网产品的兼容化、标准化以及市场化。从此以后，无线局域网随着计算机的普及得到人们越来越多的关注。无线网卡实际上是一种无线网络终端设备，它是需要在无线局域网的无线覆盖下通过无线连接网络进行上网使用的。换句话说，无线网卡就是使你的计算机可以利用无线来上网的一个装置，但是有了无线网卡，还需要一个可以连接的无线网络，因此需要配合无线路由器或者无线 AP 使用，就可以通过无线网卡以无线的方式连接无线网络来上网。

无线网卡的作用、功能与普通计算机的网卡一样，是用来连接到局域网上的。它只是一个信号收发的设备，只有在找到互联网的出口时，才能实现与互联网的连接，所有的无线网卡只能局限在已布有无线局域网的范围内。无线网卡就是不通过有线连接，采用无线信号进行连接的网卡。

无线网卡可以根据不同的接口类型来区分，第一种是USB接口的无线网卡，是最常见的；第二种是台式机专用的PCI接口的无线网卡；第三种是笔记本电脑专用的PCMCIA接口无线网卡；第四种是笔记本电脑内置的MINI-PCI无线网卡。

USB接口的无线网卡如图2-10所示。

PCI接口的无线网卡如图2-11所示。



图2-10 USB接口的无线网卡



图2-11 PCI接口的无线网卡

就如上面所说，光有无线网卡是无法连接无线网络的，还必须有无线路由器或无线AP。无线网卡就好比是接收器，无线路由相当于发射器。其实，还是需要有线的Internet线路接入到无线路由器上，再将信号转化为无线信号发射出去，由无线网卡接收。一般来说，无线路由器可以连接2～4个无线网卡，工作距离在50m范围内效果较好，否则通信质量就会变得很差。

目前，无线局域网主流的标准是IEEE 802.11n，它可大幅提升无线局域网的竞争力。随着无线局域网标准、技术快速发展，产品逐渐成熟，无线局域网的应用也日益丰富。越来越多的家庭用户开始使用无线网络，许多企业也纷纷在自己的办公大楼内布设无线局域网，同时，电信运营商对无线局域网也给予了极大关注，在机场、酒店、咖啡厅等公共区域铺设公众无线网络，给我们提供了方便的无线上网方式。

2.3.2 网桥

网桥(Bridge)是早期的两端口数据链路层网络设备，用来连接两个不同的网段。网桥的两个端口分别有一条独立的交换信道，不是共享一条背板总线，可隔离冲突域。网桥比集线器(Hub)的性能好，集线器上的各端口都共享同一条背板总线。后来，网桥被具有更多端口、同时也可隔离冲突域的交换机(Switch)所取代。

网桥的工作原理如图2-12所示。

网桥(Bridge)像一个聪明的中继器。中继器从一个网络电缆里接收信号，放大信号，将其送入下一个电缆。相比而言，网桥对从关卡上传下来的信息更敏锐一些。网桥是一种对帧进行转发的技术，根据MAC分区块，可隔离碰撞。网桥将网络的多个网段在数据链路层连接起来。

网桥也叫桥接器，是连接两个局域网的一种存储/转发设备，它能将一个大的LAN分

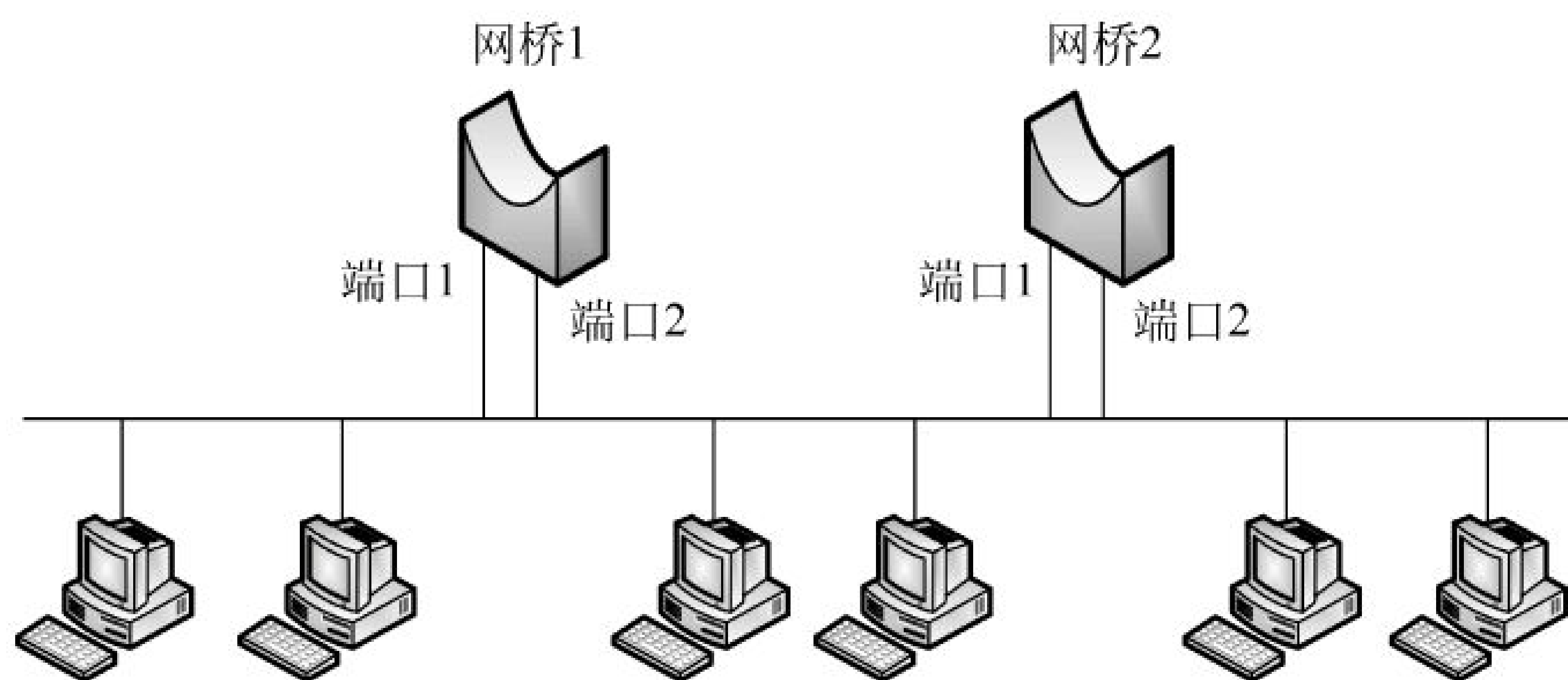


图 2-12　网桥的工作原理

割为多个网段,或将两个以上的 LAN 互联为一个逻辑 LAN,使 LAN 上的所有用户都可以访问服务器。

扩展局域网最常见的方法是使用网桥。最简单的网桥有两个端口,复杂些的网桥可以有更多的端口。网桥的每个端口与一个网段相连。

网桥将两个相似的网络连接起来,并对网络数据的流通进行管理。它工作于数据链路层,不但能扩展网络的距离或范围,而且可提高网络的性能、可靠性和安全性。网络 1 和网络 2 通过网桥连接后,网桥接收网络 1 发送的数据包,检查数据包中的地址,如果地址属于网络 1,它就将其放弃,相反,如果是网络 2 的地址,它就继续发送给网络 2,这样可利用网桥隔离信息,将同一个网络号划分成多个网段(属于同一个网络号),隔离出安全网段,防止其他网段内的用户非法访问。由于网络的分段,各网段相对独立(属于同一个网络号),一个网段的故障不会影响到另一个网段的运行。

网桥可以是专门硬件设备,也可以由计算机加装的网桥软件来实现,这时计算机上会安装多个网络适配器(网卡)。

网桥的功能在延长网络跨度上类似于中继器,然而它能提供智能化连接服务,即根据帧的终点地址处于哪一网段来进行转发和滤除。网桥对站点所处网段的了解是靠"自学习"实现的,有透明网桥、转换网桥、封装网桥和源路由选择网桥。

当使用网桥连接两段 LAN 时,网桥对来自网段 1 的 MAC 帧,首先要检查其终点地址。如果该帧是发往网段 1 上某一站的,网桥则不将帧转发到网段 2,而将其滤除;如果该帧是发往网段 2 上某一站的,网桥则将它转发到网段 2。这表明,如果 LAN1 和 LAN2 上各有一对用户在本网段上同时进行通信,显然是可以实现的。因为网桥起到了隔离作用。可以看出,网桥在一定条件下具有增加网络带宽的作用。

网桥的存储和转发功能与中继器相比有优点,也有缺点,其优点是:

使用网桥进行互连克服了物理限制,这意味着构成 LAN 的数据站总数和网段数很容易扩充。

网桥纳入存储和转发功能可使其适应于连接使用不同 MAC 协议的两个 LAN,因而构成一个不同 LAN 混连在一起的混合网络环境。

网桥的中继功能仅依赖于 MAC 帧的地址,因而对高层协议完全透明。

网桥将一个较大的 LAN 分成段,有利于改善可靠性、可用性和安全性。

网桥的主要缺点是:由于网桥在执行转发前先接收帧并进行缓冲,与中继器相比,会引

入更多时延。由于网桥不提供流量控制功能,因此在流量较大时有可能使其过载,从而造成帧的丢失。

网桥的优点多于缺点,这正是其广泛使用的原因。

网桥工作在数据链路层,将两个 LAN 连起来,根据 MAC 地址来转发帧,可以看作一个“低层的路由器”(路由器工作在网络层,根据网络地址进行转发)。

远程网桥通过一个较慢的链路(如电话线)连接两个远程 LAN,对本地网桥而言,性能比较重要,而对远程网桥而言,在长距离上可正常运行是更重要的。

2.3.3 交换机

1. 交换机的工作原理

交换机(switch)意为“开关”,是一种用于电(光)信号转发的网络设备。它可以为接入交换机的任意两个网络结点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。以太网交换机的外形如图 2-13 所示。



图 2-13 以太网交换机的外形

交换(switching)是按照通信两端传输信息的需要,用人工或设备自动完成的方法,把要传输的信息送到符合要求的相应路由上的技术的统称。交换机根据工作位置的不同,可以分为广域网交换机和局域网交换机。广域网的交换机就是一种在通信系统中完成信息交换功能的设备,应用在数据链路层。交换机有多个端口,每个端口都具有桥接功能,可以连接一个局域网或一台高性能服务器或工作站。实际上,交换机有时被称为多端口网桥。

在计算机网络系统中,交换概念的提出改进了共享工作模式。而集线器(Hub)就是一种物理层共享设备,Hub 本身不能识别 MAC 地址和 IP 地址,当同一局域网内的 A 主机给 B 主机传输数据时,数据包在以 Hub 为架构的网络上是以广播方式传输的,由每台终端通过验证数据报头的 MAC 地址来确定是否接收。也就是说,在这种工作方式下,同一时刻网络上只能传输一组数据帧的通信,如果发生碰撞,还得重试。这种方式就是共享网络带宽。通俗地说,普通集线器是不带管理功能的,只有一根连线接入,并直接连接到其余所有的计算机上。

交换机工作于 OSI 参考模型的第二层,即数据链路层。交换机内部的 CPU 会在每个端口成功连接时,通过将 MAC 地址和端口对应,形成一张 MAC 表。在今后的通信中,发往该 MAC 地址的数据包将仅送往其对应的端口,而不是所有的端口。因此,交换机可用于划分数据链路层广播,即冲突域;但它不能划分网络层广播,即广播域。

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机所有的端口都挂接在这条背部总线上,控制电路收到数据包以后,处理端口会查找内存中的地址对照表,以确定目的 MAC(网卡的硬件地址)的 NIC(网卡)挂接在哪个端口上,通过内部交换矩阵迅速将数据包传送到目的端口,目的 MAC 若不存在,就广播到所有的端口,接收端口回应后,交换机会“学习”新的 MAC 地址,并把它添加到内部 MAC 地址表中。使用交换机也可以把网络“分段”,通过对照 IP 地址表,交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发,可以有效地减少冲突域,但它不能划分网络层广播,即广播域。

交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的物理网段(注：非 IP 网段)，连接在其上的网络设备独自享有全部带宽，无须同其他设备竞争使用。当结点 A 向结点 D 发送数据时，结点 B 可同时向结点 C 发送数据，而且这两个传输都享有网络的全部带宽，都有自己的虚拟连接。假使这里使用的是 10Mb/s 的以太网交换机，那么该交换机这时的总流通量就等于 2×10Mb/s=20Mb/s，而使用 10Mb/s 的共享式 Hub 时，一个 Hub 的总流通量也不会超出 10Mb/s。总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据帧功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

2. 交换机的主要功能

交换机是一种基于 MAC 地址识别，能完成数据包封装并转发的网络互联设备。交换机主要实现地址学习、帧的转发和过滤、消除回路等功能。

1) 地址学习

交换机会自动学习每个端口相连设备的 MAC 地址，并将 MAC 地址同相应的端口建立映射，缓存在 MAC 地址表中。交换机每收到一个数据信息都查看地址表，有映射记录就按照地址表中对应的信息转发；没有映射记录就转发给自己以外的所有端口，并记录下端口和网卡地址的映射信息，直到连接到交换机的所有计算机都发送过数据之后，MAC 映射地址表最终建立完整。

2) 帧的转发和过滤

当一个帧到达交换机后，交换机通过查找 MAC 地址表来决定如何转发数据帧。如果目的 MAC 地址存在，则将数据帧转发到相应的端口。如果在 MAC 地址表中找不到目的地址，则将数据帧向所有端口转发。

交换机首先将整帧数据都接收下来，经过校验无错误后放入缓存，然后再将其转发出去。帧通过交换机的转发时延随帧长度的不同而变化。如果在差错检测的过程中发现数据帧出错，则将这个错误的数据帧丢弃。

3) 消除回路

当网络的范围不断扩展，出现多台交换机互相连接时，经常会将交换机互相连接成一个交换链路环，以保持网络的冗余性和稳定性，使得当某一台交换机发生故障时，链路不会中断。但是，互相连接形成的回路很容易产生广播风暴、多帧复制和 MAC 地址表不稳定等现象。

当交换机包含冗余回路时，以太网交换机通过生成树协议避免回路的产生，同时允许存在后备路径。

3. 第三层交换机

第三层交换机因为工作于 OSI/RM 模型的网络层，所以具有路由功能，它是将 IP 地址信息提供给网络路径选择，并实现不同网段间数据的线速交换。当网络规模较大时，可以根据特殊应用需求划分为小面独立的 VLAN 网段，以减少广播造成的影响。

第三层交换机同样是对应于 OSI/RM 模型的第三层——网络层来定义的。也就是说，这类交换机可以工作在网络层，它比第二层交换机更高档，功能更强。

通常，这类交换机采用模块化结构，以适应灵活配置的需要。

在大中型网络中，第三层交换机已经成为基本配置设备。

三层交换机就是具有部分路由器功能的交换机。三层交换机的最重要目的是加快大型局域网内部的数据交换，所具有的路由功能也是为这个目的服务的，能够做到一次路由，多次转发。对于数据包转发等规律性的过程，由硬件高速实现，而像路由信息更新、路由表维护、路由计算、路由确定等功能，由软件实现。

4. 交换机的管理方式

交换机可以通过以下 3 种方式进行管理：通过 RS-232 串行口管理、通过网络浏览器管理和通过网络管理软件管理。

1）通过 RS-232 串行口管理

可网管交换机附带了一条串行电缆，供交换机管理使用。先把串行电缆的一端插在交换机背面的串行口里，另一端插在普通计算机的串行口里，然后接通交换机和计算机电源。Windows XP 操作系统中提供了“超级终端”程序。启动“超级终端”程序，设定好连接参数后，就可以通过串行口对交换机进行管理(注：详见本书第 4.3 节)了。这种方式并不占用交换机的带宽，因此称为“带外管理”。

在这种管理方式下，交换机提供了一个命令行界面。可以输入交换机的管理命令，按 Enter 键执行相应的命令。不同品牌的交换机，命令集是不同的，甚至同一品牌不同型号的交换机，其命令也略有不同。

2）通过网络浏览器管理

交换机也可以通过网络浏览器(Web)进行管理，但是必须为交换机分配一个 IP 地址。这个 IP 地址除了供管理交换机使用之外，并没有其他用途。在默认状态下，交换机没有 IP 地址，必须通过串口或其他方式指定一个 IP 地址之后，才能启用这种管理方式。

使用网络浏览器管理交换机时，交换机相当于一台 Web 服务器，只是网页文件并不储存在硬盘里面，而是在交换机的 NVRAM(非易失随机存取存储器)里面，通过浏览器可以访问 NVRAM 里面的网页文件。当管理员在浏览器中输入交换机的 IP 地址时，交换机就像一台服务器一样把网页传递给计算机，此时给用户的感觉就像在访问一个网站一样。这种方式占用交换机的带宽，因此称为“带内管理”。

如果用户要管理交换机，只要单击网页中相应的功能项，在文本框或下拉列表中改变交换机的参数就可以了。Web 管理这种方式可以在局域网上进行，也可以在互联网上进行，实现远程管理。

3）通过网络管理软件管理

交换机也可以通过软件进行管理，这种管理方式主要是以简单网络管理协议(Simple Network Management Protocol，SNMP)实现的。SNMP 是一整套的符合国际标准的网络设备管理规范。凡是遵循 SNMP 的设备，均可以通过网管软件来管理。只在一台网管工作站上安装一套 SNMP 网络管理软件，通过局域网就可以很方便地管理网络上的交换机、路由器和服务器等网络设备了。

2.4 网络层设备

网络层是 OSI 参考模型中的第三层，介于传输层和数据链路层之间，它在数据链路层提供的两个相邻端点之间的数据帧的传送功能上，进一步管理网络中的数据通信，将数据设

法从源端经过若干个中间结点传送到目的端，从而向传输层提供最基本的端到端的数据传送服务。主要内容有：虚电路分组交换和数据报分组交换、路由选择算法、阻塞控制方法、X.25 协议、综合业务数据网(ISDN)、异步传输模式(ATM)及网际互联原理与实现。

网络层互联的设备是路由器(Router)。网络层互联主要解决路由选择、拥塞控制、差错处理与分段技术等问题。如果网络层协议相同，则互联主要解决路由选择问题。如果网络层协议不同，则需要使用支持多种不同协议的路由器。用路由器实现网络互联时，允许互连的第三层以下的各层的网络协议不同。路由器的外形如图 2-14 所示。



图 2-14　路由器的外形

1. 路由器的主要功能

简单地说，路由器的主要功能是实现不同网络之间的连接，并实现不同网络之间的信息传输。

1) 连通不同的网络

从过滤网络流量的角度看，路由器的作用与交换机和网桥非常相似。但是，与工作在数据链路层，从物理上划分网段的交换机不同，路由器使用专门的软件协议从逻辑上对整个网络进行划分。例如，一台支持 IP 的路由器可以把网络划分成多个子网段，只有指向特殊 IP 地址的网络数据，才可以通过路由器。对于每个接收到的数据包，路由器都会重新计算其校验值，并写入新的物理地址。因此，使用路由器转发和过滤数据的速度往往要比只查看数据包物理地址的交换机慢。但是，对于那些结构复杂的网络，使用路由器可以提高网络的整体效率。路由器的另外一个优势是可以自动过滤网络广播。

2) 信息传输

有的路由器仅支持单一协议，但大部分路由器可以支持多种协议的传输，即多协议路由器。由于每种协议都有自己的规则，所以要在一个路由器中完成多种协议的算法，势必会降低路由器的性能。路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略(即路由算法)是路由器的关键。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表(Routing Table)，供路由选择时使用。路由表可以分为静态路由表和动态路由表。

静态路由表：网络管理员事先设置好固定的路由表称为静态(static)路由表。

动态路由表：动态(dynamic)路由表是路由器根据网络系统的运行情况而自动调整的路由表。

路由器是一种多端口设备，它可以连接不同传输速率并运行于各种环境的局域网和广域网，也可以采用不同的协议。路由器属于第三层设备，即工作在 OSI 参考模型的第三层，实现从一个网段到另一个网段的数据传输，也能实现从一种网络向另一种网络的数据传输，即网络互联、数据处理、网络管理。

(1) 网络互联：路由器支持各种局域网和广域网接口，主要用于互联局域网和广域网，实现不同网络互相通信。

(2) 数据处理：提供包括分组过滤、分组转发、优先级、复用、加密、压缩和防火墙等功能。

(3) 网络管理：路由器提供包括路由器配置管理、性能管理、容错管理和流量控制等

功能。

2. 路由的基本概念

路由是指把数据从一个地方传送到另一个地方的行为和动作，而路由器正是执行这种行为动作的机器，它的英文名称为 Router，是一种连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读懂”对方的数据，从而构成一个更大的网络。

为了完成“路由”的工作，路由器中保存着各种传输路径的相关数据——路由表，供路由选择时使用。路由表中保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。路由表可以是由网络管理员固定设置好的，也可以由系统动态修改，即可以由路由器自动调整。在路由器中涉及两个有关地址的名字概念：静态路由表和动态路由表。路由器根据路由选择协议（Routing Protocol）提供的功能，自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

3. 路由协议

路由协议工作在路由器上，用来确定到达网络数据包传输的路径，与汽车上常用的全球定位系统（GPS）导航仪相似。路由协议在计算机网络中起着导航的作用。路由协议工作在网络层。常用的路由协议包括 RIP、IGRP（Cisco 私有协议）、EIGRP（Cisco 私有协议）、OSPF 协议、IS-IS 协议、BGP 等。

路由协议作为 TCP/IP 协议簇中的重要成员之一，其选路过程实现的好坏会影响整个 Internet 网络的效率。按应用范围的不同，路由协议可分为两类：内部网关协议和外部网关协议。

在一个自治系统（Autonomous System，AS）内的路由协议称为内部网关协议（Interior Gateway Protocol，IGP）。这里，自治系统是指一个互联网络，就是把整个 Internet 划分为许多较小的网络单位，这些小的网络有权自主地决定在本系统中应采用何种路由协议。而自治系统之间的路由协议称为外部网关协议（Exterior Gateway Protocol，EGP）。这里，网关是指路由器。

常用的内部网关路由协议有以下几种：RIPv1、RIPv2、IGRP、EIGRP、IS-IS 和 OSPF。其中前 3 种路由协议采用的是距离矢量算法，IS-IS 和 OSPF 采用的是链路状态算法，EIGRP 是结合了链路状态算法和距离矢量算法的 Cisco 私有路由协议。对于小型网络，采用基于距离矢量算法的路由协议易于配置和管理，且应用较为广泛。但对于大型网络，距离矢量算法固有的环路问题变得更难解决，所占用的带宽也迅速增长，以至于网络无法承受。因此，对于大型网络，采用链路状态算法的 OSPF 协议和 IS-IS 协议较为有效，并且得到了广泛的应用。IS-IS 与 OSPF 在质量和性能上的差别并不大，但 OSPF 更适用于 IP，较 IS-IS 更具有活力。IETF 始终在致力于 OSPF 的改进工作，其修改节奏要比 IS-IS 快得多，这使得 OSPF 成为应用广泛的一种路由协议。不论是传统的路由器设计，还是即将成为标准的 MPLS（多协议标记交换），均将 OSPF 视为必不可少的路由协议。

外部网关协议最初采用的是 EGP。EGP 是为一个简单的树形拓扑结构设计的。越来越多的用户和网络加入 Internet，给 EGP 带来很多的局限性。为了摆脱 EGP 的局限性，IETF（国际互联网工程任务组）边界网关协议工作组制定了标准的边界网关协议——BGP。

2.5　应用层设备

应用层设备主要分为服务器和防火墙两大类。服务器(如邮件服务器和网站服务器等)提供信息资源,防火墙则用于保护企业内部网络的安全。

2.5.1　服务器

服务器(Server)也称伺服器,是提供计算服务的设备。由于服务器需要响应服务请求,并进行处理,因此一般来说服务器应具备承担服务并且保障服务的能力。

服务器的构成包括处理器、硬盘、内存、系统总线等,和通用的计算机架构类似,但是由于需要提供高可靠的服务,因此在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面要求较高。

在网络环境下,服务器根据提供的服务类型不同,分为文件服务器、数据库服务器、应用程序服务器和 Web 服务器等。

1. 服务器硬件

服务器作为硬件来说,通常指那些具有较高计算能力,能够提供给多个用户使用的计算机。服务器与 PC 的不同点很多,例如,PC 在一个时刻通常只为一个用户服务,是通过终端给用户使用的,而服务器是通过网络给客户端用户使用的。

和普通的 PC 相比,服务器需要连续工作 7×24 小时。这就意味着需要服务器的性能更加稳定。

根据不同的计算能力,服务器又分为工作组级服务器、部门级服务器和企业级服务器。服务器操作系统是指运行在服务器硬件上的操作系统。服务器操作系统需要管理和充分利用服务器硬件的计算能力,并提供给服务器硬件上的软件使用。

2. 服务器的硬件结构

服务器系统的硬件构成与我们平常接触的计算机有许多相似之处,主要的硬件构成同样包括以下几个主要部分:中央处理器(CPU)、内存、芯片组、I/O 总线、I/O 设备、电源、机箱和相关软件。

例如,整个服务器系统就像一个人,处理器就是服务器的大脑,而各种总线就像是分布于全身肌肉中的神经,芯片组就像是骨架,而 I/O 设备就像是通过神经系统支配的人的手、眼睛、耳朵和嘴;而电源系统就像是血液循环系统,它将能量输送到身体的所有地方。

在信息系统中,服务器主要应用于数据库和 Web 服务,而 PC 主要应用于桌面计算和网络终端,设计根本出发点的差异决定了服务器应该具备比 PC 更可靠的持续运行能力、更强大的存储能力和网络通信能力、更快捷的故障恢复功能和更广阔的扩展空间,同时,对数据相当敏感的应用还要求服务器提供数据备份功能。而 PC 在设计上则更加重视人机接口的易用性、图像和 3D 处理能力及其他多媒体性能。

3. 服务器的中央处理器(CPU)

服务器的 CPU 仍按 CPU 的指令系统来区分,通常分为 CISC 型 CPU 和 RISC 型 CPU 两类,后来又出现了一种 64 位的超长指令字(Very Long Instruction Word,VLIW)指令系统的 CPU。

1）CISC 型 CPU

CISC 是英文 Complex Instruction Set Computer 的缩写，中文意思是“复杂指令集”，它是指英特尔生产的 X86(Intel CPU 的一种命名规范)系列 CPU 及其兼容 CPU(其他厂商如 AMD、VIA 等生产的 CPU)，它基于 PC(个人计算机)体系结构。这种 CPU 一般都是 32 位的结构，所以我们也把它称为 IA-32 CPU。(IA 指 Intel 架构)。CISC 型 CPU 主要有 Intel 的服务器 CPU 和 AMD 的服务器 CPU 两类。

2）RISC 型 CPU

RISC 是英文 Reduced Instruction Set Computer 的缩写，中文意思是“精简指令集”。它是在 CISC 指令系统基础上发展起来的，相对于 CISC 型 CPU，RISC 型 CPU 不仅精简了指令系统，还采用了一种“超标量和超流水线结构”，架构在同等频率下。采用 RISC 架构的 CPU 比 CISC 架构的 CPU 性能高很多，这是由 CPU 的技术特征决定的。RISC 型 CPU 与 Intel 和 AMD 的 CPU 在软件和硬件上都不兼容。

2.5.2 防火墙

防火墙(Fire Wall)指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关(Security Gateway)，从而保护内部网免受非法用户侵入。防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成。防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入/流出的所有网络通信和数据包均要经过此防火墙。防火墙的工作原理如图 2-15 所示。

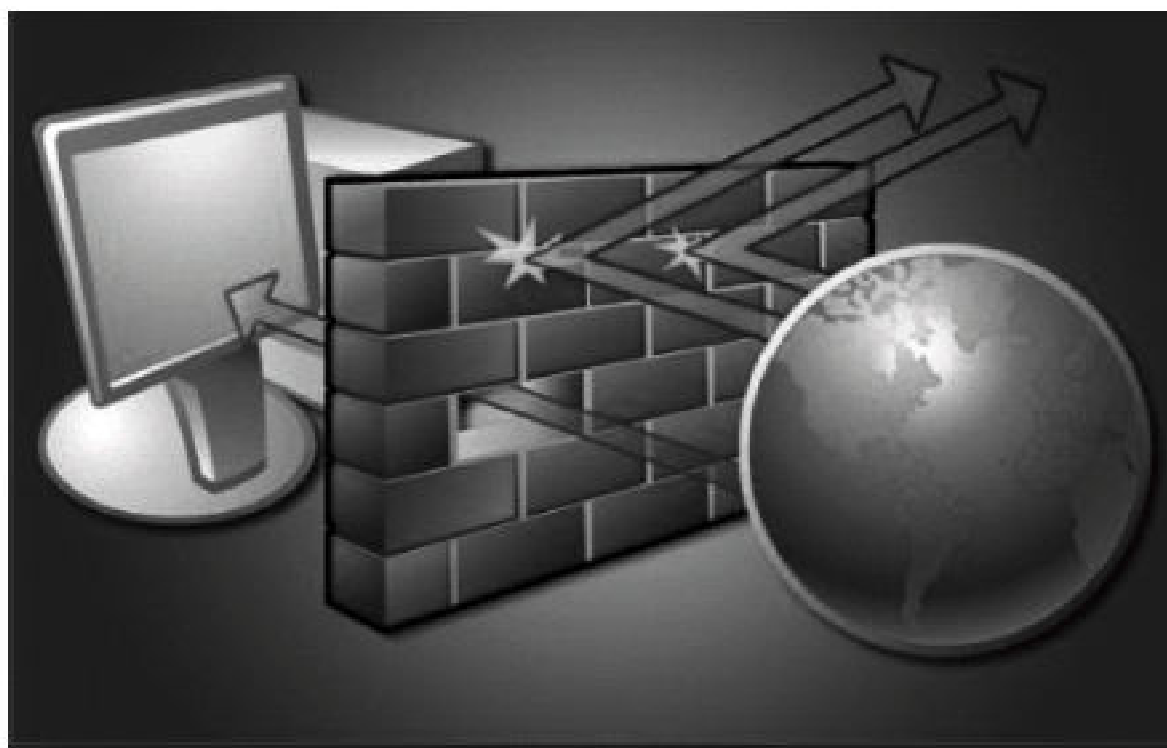


图 2-15 防火墙的工作原理

在网络中，所谓的“防火墙”，是指一种将内部网和公众访问网(如 Internet)分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问 Internet，Internet 上的人也无法和公司内部的人进行通信。

防火墙从诞生开始，已经历了 4 个发展阶段：基于路由器的防火墙、用户化的防火墙工具套、建立在通用操作系统上的防火墙和具有安全操作系统的防火墙。常见的防火墙属于具有安全操作系统的防火墙，如 NETEYE、NETSCREEN 和 TALENTIT 等。

从结构上分，防火墙有两种：代理主机结构和路由器＋过滤器结构。

从原理上分，防火墙可以分成 4 种类型：特殊设计的硬件防火墙、数据包过滤型、电路层网关和应用级网关。安全性能高的防火墙系统都组合运用多种类型防火墙，构筑多道防火墙"防御工事"。

2.6　本章总结

本章讨论了网络互联涉及的各种传输介质和设备，包括各种有线和无线传输介质、物理层设备、数据链路层设备、网络层设备和应用层设备等。

有线传输介质是指在两个通信设备之间实现的物理连接部分，它能将信号从一端传输到另一端。有线传输介质主要有双绞线、同轴电缆和光纤。双绞线和同轴电缆传输电信号，光纤传输光信号。

无线传输介质指我们周围的自由空间。我们利用无线电波在自由空间的传播可以实现多种无线通信。在自由空间传输的电磁波根据频谱可分为无线电波、微波、红外线和激光等，信息被加载在电磁波上进行传输。

连接器是连接电缆与网络设备的硬件。网络设备可以是一个文件服务器、工作站、交换机或打印机。每种网络介质都对应一种特定类型的连接器。

双绞线简称 TP，可将一对以上的双绞线封装在一个绝缘外套中，为了降低信号的干扰程度，电缆中的每对双绞线一般由两根绝缘铜导线相互扭绕而成的，也因此把它称为双绞线。双绞线可以分为非屏蔽双绞线（Unshielded Twisted Pair，UTP）和屏蔽双绞线（Shielded Twisted Pair，STP）两大类。

同轴电缆由一根空心的外圆柱导体和一根位于中心轴线的内导体组成，两者之间用绝缘材料隔开，具有抗干扰能力强、连接简单等特点，信息传输速度可达每秒几百兆位，是中、高档局域网的首选传输介质。

光纤是由一组光导纤维组成的用来传播光束的、细小而柔韧的传输介质。应用光学原理，由光发送机产生光束，将电信号变为光信号，再把光信号导入光纤，在另一端由光接收机接收光纤上传来的光信号，并把它变为电信号，经解码后再处理。

光纤可以分为单模光纤和多模光纤。

常用的无线传输介质有微波、红外线、无线电波。

微波是指频率为 300MHz～300GHz 的电磁波，是无线电波中一个有限频带的简称，即波长在 1m（不含 1m）到 1mm 之间的电磁波，是分米波、厘米波、毫米波的统称。

红外线是太阳光线中众多不可见光线中的一种，由德国科学家霍胥尔于 1800 年发现。红外线的波长大于可见光线，波长为 0.75～15.0μm。红外线可分为 3 类，即近红外线，波长在 0.75～1.50μm 之间；中红外线，波长在 1.50～6.0μm 之间；远红外线，波长在 6.0～15.0μm 之间。

无线电波是指在自由空间（包括空气和真空）传播的射频频段的电磁波。无线电技术是通过无线电波传播声音或其他信号的技术。

中继器（Repeater，RP）是工作在物理层上的连接设备，适用于完全相同的两类网络的互联，主要功能是通过对数据信号的重新发送或者转发，来扩大网络传输的距离。中继器是对信号进行再生和还原的网络设备，即工作在 OSI 模型中物理层的设备。

集线器的英文为 Hub。Hub 是“中心”的意思，集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有结点集中在以它为中心的结点上。它也工作于 OSI 参考模型最低层，即“物理层”。

无线 AP 是使用无线设备（如手机、笔记本电脑和平板电脑等）进入有线网络的接入点，主要用于宽带家庭、大楼内部、校园内部、园区内部以及仓库、工厂等需要无线监控的地方，典型距离覆盖几十米至上百米。

数据链路层在物理层提供的服务的基础上向网络层提供服务，其最基本的服务是将源自网络层的数据可靠地传输到相邻结点的目标机网络层。常用的数据链路层设备有网卡、网桥、交换机等。

网卡也称为网络适配器，是工作在数据链路层的网络组件。它是局域网中连接计算机和传输介质的接口，不仅能实现与局域网传输介质之间的物理连接和电信号匹配，还涉及帧的发送与接收、帧的封装与拆封、介质访问控制、数据的编码与解码以及数据缓存的功能等。网卡可以分为有线网卡和无线网卡。

网桥（Bridge）是早期的两端口数据链路层网络设备，用来连接两个不同的网段。网桥的两个端口分别有一条独立的交换信道，不是共享一条背板总线，可隔离冲突域。

交换机（Switch）意为“开关”，是一种用于电（光）信号转发的网络设备。它可以为接入交换机的任意两个网络结点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。

网络层互联的设备是路由器（Router）。网络层互联主要解决路由选择、拥塞控制、差错处理与分段技术等问题。如果网络层协议相同，则互联主要解决路由选择问题。如果网络层协议不同，则需要使用支持多种不同协议的路由器。

路由协议工作在路由器上，用来确定到达网络数据包传输的路径，其工作原理与汽车上常用的全球定位系统（GPS）相似。路由协议在计算机网络中起着导航的作用。路由协议工作在网络层，分为静态路由协议和动态路由协议。常用的动态路由协议包括 RIP、IGRP（Cisco 私有协议）、EIGRP（Cisco 私有协议）、OSPF、IS-IS 协议、BGP 等。

应用层设备主要分为服务器和防火墙两大类。服务器（如邮件服务器和网站服务器等）提供信息资源，防火墙则用于保护企业内部网络的安全。

复习思考题

1. 常用的双绞线使用什么型号的连接器？
2. 什么是 UTP？什么是 STP？UTP 和 STP 各有什么特点？
3. 请列表说明双绞线的 568A 和 568B 接线规范。
4. 请简要说明同轴电缆的内部结构和特点。
5. 什么是单模光纤？什么是多模光纤？它们各有什么特点？
6. 常用的无线传输介质有哪些？它们各有什么特点？
7. 什么是集线器？集线器按结构和功能分类，可以分为哪些类型？
8. 什么是无线接入点？无线接入点的作用是什么？
9. 有线网卡的工作原理是什么？其基本功能是什么？

10．无线网卡的工作原理是什么？无线网卡有哪些标准？
11．请比较网桥与中继器的异同点。
12．交换机的工作原理是什么？其主要功能是什么？
13．什么是第三层交换机？
14．交换机的管理方式有哪些？
15．路由器的主要功能是什么？
16．什么是路由协议？
17．常用的路由协议有哪些？
18．请简要说明服务器系统的硬件结构。
19．什么是防火墙？防火墙分为哪些类型？

第3章 路由器技术基础

CHAPTER 3

3.1 认识路由器

路由器(Router)是连接国际互联网中各个局域网、广域网的核心设备,它会根据信道的实际情况自动选择和设定路由,以最佳的路径按先后顺序发送数据包。路由器是互联网络的枢纽,就像“交通警察”一样管理着网络。目前,路由器已经广泛应用于各行各业,各种不同档次的路由器产品已成为实现骨干网内部连接、骨干网间互联和骨干网与国际互联网互联互通业务的主力军。路由器和交换机之间的主要区别就是交换机工作在OSI参考模型的第二层(数据链路层),而路由器则工作在第三层,即网络层。这一区别决定了路由器和交换机在传输信息的过程中需要使用不同的控制协议,所以说它们两者实现各自功能的工作原理是不同的。

生产路由器的厂商有美国的思科(Cisco)公司、瞻博(Juniper)公司和中国的华三(H3C)公司等。Cisco公司的7609-S型机柜式路由器如图3-1所示。

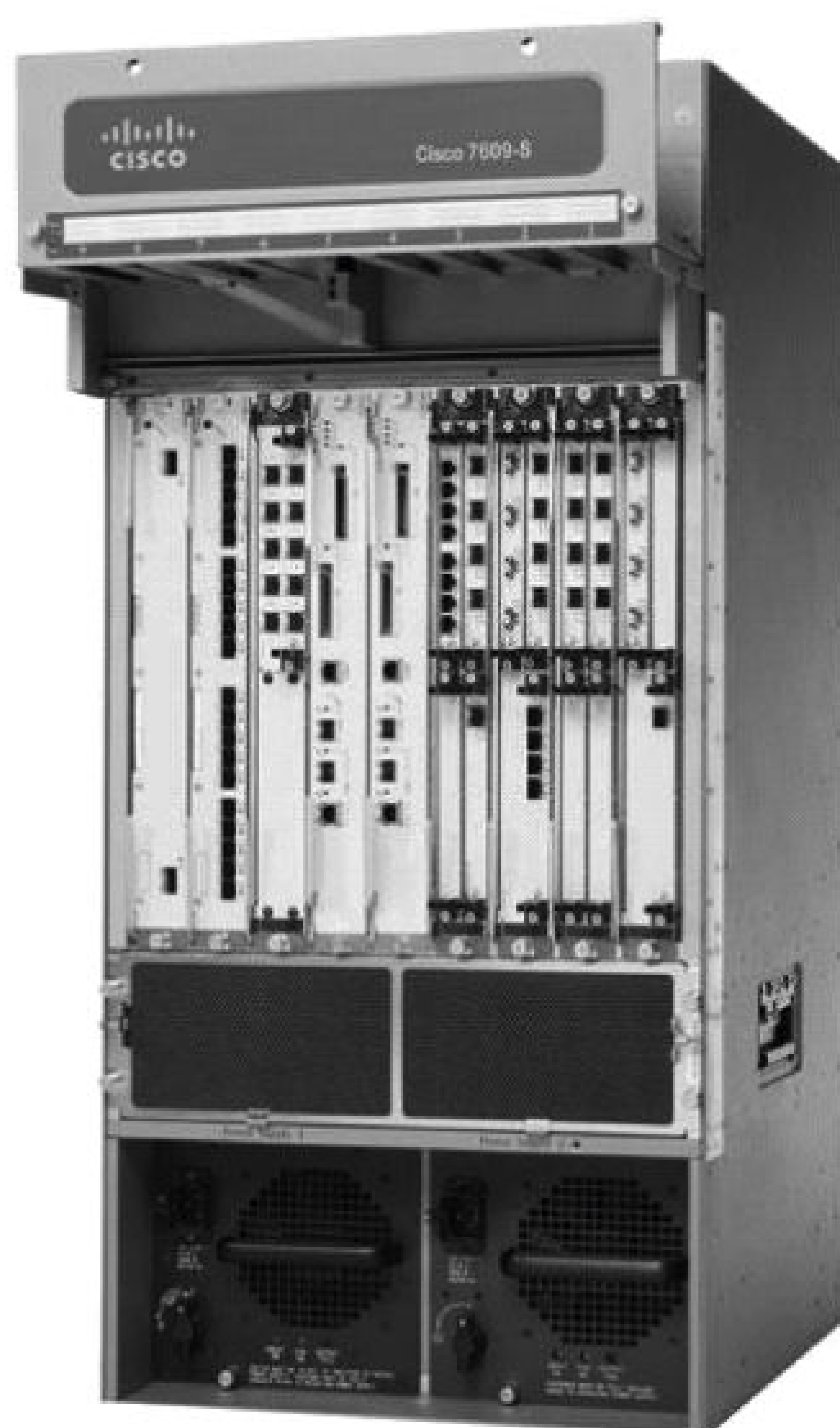


图3-1 Cisco公司的7609-S型机柜式路由器

Cisco公司是全球领先的网络解决方案供应商。组成互联网和数据传送的路由器、交换机等网络设备市场几乎都由Cisco公司控制。

中国的华三(H3C)公司也是一家优秀的网络互联设备生产商。NE系列路由器为华三面向运营商数据通信网络的高端路由器产品,覆盖骨干网、城域网的P/PE位置,帮助运营商应对网络带宽快速增长的压力,支持RIP、OSPF、BGP、IS-IS等单播路由协议和IGMP、PIM、MBGP、MSDP等多播路由协议,支持多种路由策略。华三公司的20系列路由器如图3-2所示。



图3-2　华三公司的20系列路由器

由于华三公司在国内拥有较高的知名度,因此华三公司也建立了和Cisco公司相似的培训认证体系,如HCNE(华为认证网络工程师)对应CCNA、HCSE对应CCNP、H3CIE对应CCIE。

3.2　路由器的硬件结构

和其他计算机产品一样,路由器也是由硬件和软件组成的。路由器硬件包括中央处理器(CPU)、只读存储器(ROM)、随机存取存储器(RAM)、闪存(Flash)、非易失性存储器(NVRAM)、控制端口(Console)和辅助控制端口(AUX)、以太网接口、串行接口、扩展接口等;而路由器的主要软件是iOS。与其他类型的计算机产品不同的是,路由器硬件一般并不包含硬盘。路由器的硬件组成如图3-3所示。

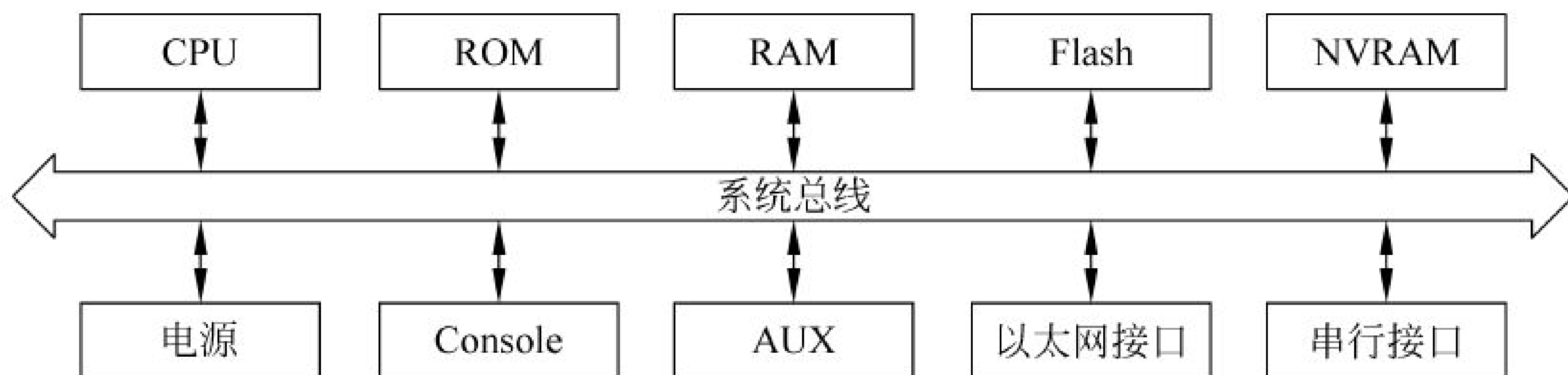


图3-3　路由器的硬件组成

1. 中央处理器

中央处理器(Central Processing Unit,CPU)是一块超大规模的集成电路,是一台计算机的运算核心(Core)和控制核心。它的功能主要是解释并运行计算机指令以及处理计算机软件中的数据。

Cisco路由器的中央处理器(CPU)采用Motorola 68030或Orion/R4600集成电路芯片,主要负责配置和管理路由表和数据包的转发工作等。

无论在中低端路由器,还是在高端路由器中,CPU都是路由器的核心。通常,在中低端路由器中,CPU负责交换路由信息、路由表查找以及转发数据包。在高端路由器中,通常包转发和查表由ASIC芯片完成,CPU只实现路由协议、计算路由以及分发路由表。由于技术的发展,路由器中的许多工作都可以由硬件实现(专用芯片)。CPU性能并不完全反映路由器性能。路由器性能由路由器吞吐量、时延和路由计算能力等指标体现。

2. 只读存储器

只读存储器(Read-Only Memory,ROM)是一种只能读取代码或数据的固态半导体存储器。其特性是：一旦储存资料,就无法再将之改变或删除,通常用于保存代码,这些代码不会因为电源关闭而消失。

路由器中的只读存储器主要用来储存厂家生产路由器产品时事先固化写入的程序代码,主要包括系统加电自检代码(POST)、系统引导区代码。

3. 随机存取存储器

随机存取存储器(Random Access Memory,RAM)又称作"随机存储器",是与 CPU 直接交换数据的内部存储器,也叫主存(内存)。它可以随时读写,而且速度很快,通常作为操作系统或其他正在运行中的程序的临时数据存储媒介。

随机存储器可以按需随意取出或存入数据,且存取的速度与存储单元的位置无关。这种存储器在断电时将丢失其存储内容,故主要用于存储短时间使用的程序。按照存储单元的工作原理,随机存储器又分为静态随机存储器(Static RAM,SRAM)和动态随机存储器(Dynamic RAM,DRAM)。

在路由器运行期间,RAM 中除了包含当前正在运行的配置文件、正在执行的代码、操作系统程序和一些相关的临时数据外,还包含路由表、ARP 表、缓存待发送的数据包等。

4. 闪存

闪存(Flash)是一种长寿命的非易失性(在断电情况下仍能保持所存储的数据信息)的存储器,数据删除时并不是以单个字节为单位,而是以固定的区块为单位,区块大小一般为256KB～20MB。闪存是电子可擦除只读存储器(E^2PROM)的变种,与 E^2PROM 不同的是,E^2PROM 能在字节水平上进行删除和重写,而不是整个芯片擦写,而闪存的大部分芯片需要以区块为单位删除数据。由于闪存在断电时仍能保存数据,故通常用来保存设置信息。

由于闪存在重新启动或关机之后仍能保存数据,因此路由器的闪存相当于计算机中的硬盘,主要用作存放操作系统,甚至可以存放多个版本的 iOS,对升级系统有利。

闪存中存放的是路由器的操作系统 iOS(Interconnection working Operation System),例如典型的 Cisco 的路由器操作系统,就是用压缩格式的映像文件存放在路由器 Flash 中的。

5. 非易失性存储器

非易失性存储器(Non Volatile RAM,NVRAM)是可读可写的,在系统重新启动或者关机之后仍能保存数据。NVRAM 存取数据的速度很快,但是成本较高,仅用于保存启动配置(Startup-Config)文件,其容量较小,通常只有 32～128KB。

6. 路由器接口

目前,主流的局域网技术是以太网技术,因此路由器提供 10M 的以太网接口、100M 的快速以太网接口、千兆以太网接口和万兆以太网接口等。此外,路由器还可以提供同步串行接口、异步串行接口和高速同步串行接口、光纤接口等。路由器的典型接口如图 3-4 所示。

7. 控制端口

控制端口(Console)与计算机的连接如图 3-5 所示。

路由器并没有自己专用的键盘、鼠标与显示器等输入/输出设备,因此为了便于对路由器进行初始化配置和管理,路由器通常提供两个用于管理的接口：控制端口(Console)和辅助端口(AUX)。当对路由器进行初始化配置时,必须使用这两个管理端口中的其中一个。

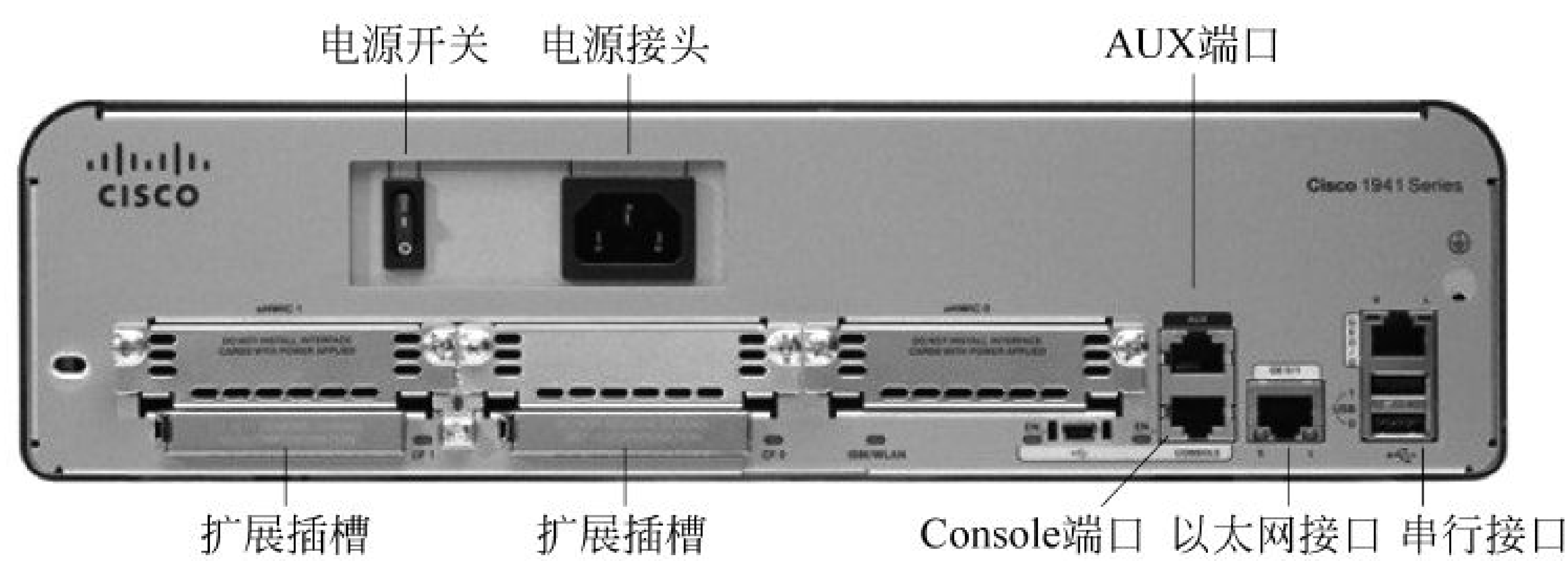


图 3-4　路由器的典型接口

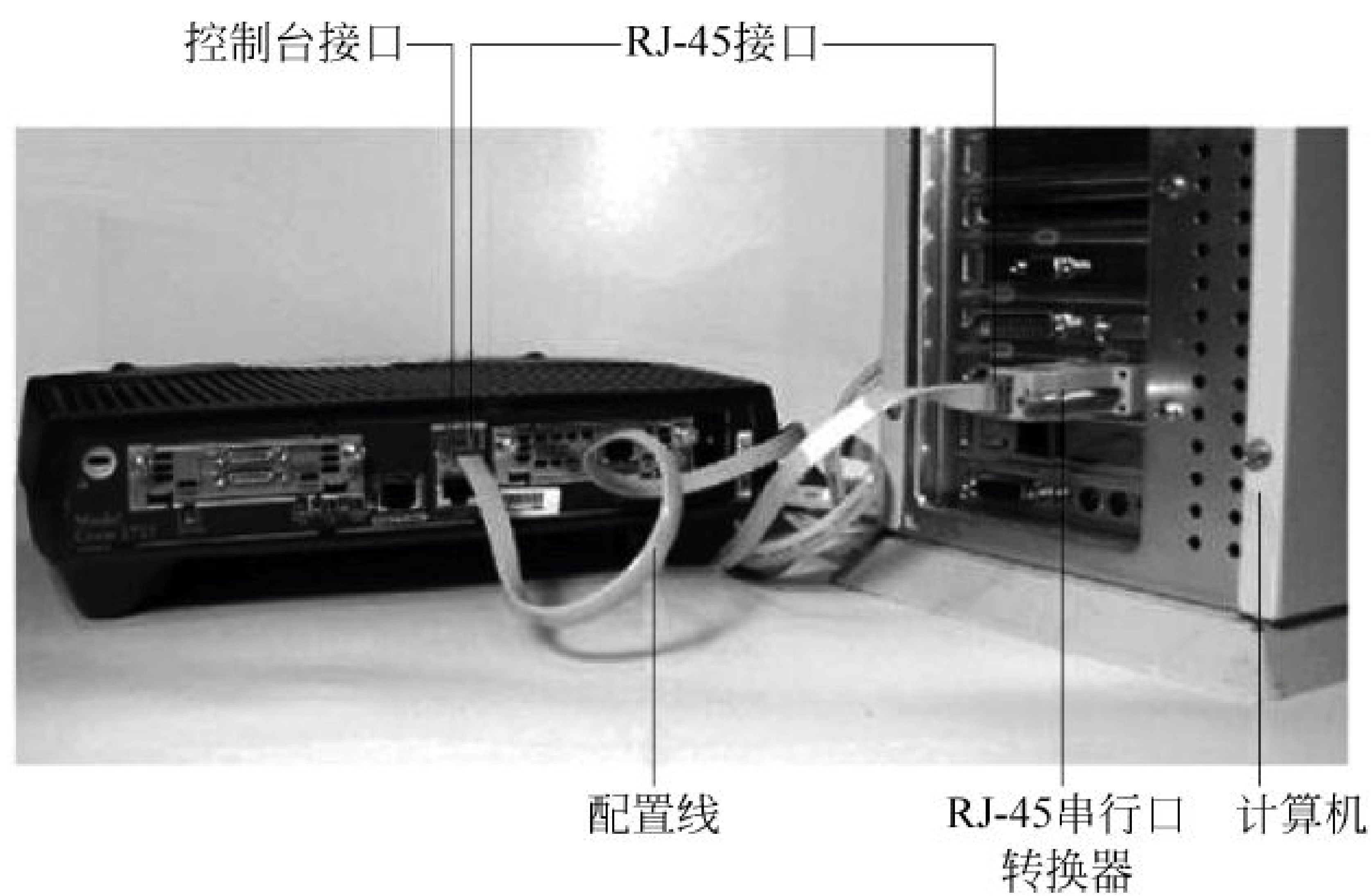


图 3-5　控制端口与计算机的连接

几乎所有的路由器都有 Console 端口，但是并非所有的路由器上都有 AUX 端口。Console 端口是一个 EIA/TIA-232 异步串行接口，通过计算机上的称为“超级终端”的管理软件对直接连接的路由器进行配置和管理。

因为许多笔记本电脑没有串行口(COM 口)，所以当用笔记本电脑充当路由器的控制设备时，需要另外购买一条 USB 转为串行口的转接线，将该线 USB 端连接笔记本电脑的 USB 端口，另一端连接控制线，再将控制线接入到路由器的 Console 端口。

3.3　路由器的软件

与其他计算机系统一样，软件也是路由器的重要组成部分。路由器的软件主要包括自举程序、路由器操作系统、配置文件和实用管理程序等。

1. 自举程序

所有的计算机系统在启动时首先都需要运行固化在 ROM 中的自举程序来引导操作系统。路由器也不例外，启动时同样需要自举程序来加载路由器操作系统。自举程序是固化在 ROM 中的软件，又称为固件。自举程序的功能是在路由器加电后完成有关的初始化工作，并负责向内存装入操作系统代码。Cisco 的自举程序称为 BootStrap，华三(H3C)的自举程序称为 BootROM。

2. 路由器操作系统

除了硬件以外,每个路由器都由路由器操作系统来统一指挥和调度路由器各个硬件的运行。路由器厂商对路由器操作系统的称谓也并不相同。下面对思科(Cisco)、瞻博(Juniper)和华三(H3C)这三家公司的路由器操作系统进行简要介绍。

1) iOS

互联网操作系统(Internet working Operating System,iOS)是思科公司为其网络产品开发的操作系统。用户通过命令行人机界面对网络设备进行功能设置,提供的功能大致为以下几点:网络设备及连接端口的功能首选项设置、运行网络协议与网络功能设备之间的数据传输安全管理设置。

Cisco 是一个与硬件分离的系统软件,随着计算机网络技术的不断发展,iOS 可以动态地升级,以适应不断进步的技术(硬件和软件)。iOS 可以被视作一个网际互联中枢:一个高度智能的网络管理员,负责管理和控制复杂的分布式的网络资源。

Cisco 公司的路由器和交换机系列产品使用的操作系统都称为 iOS。Cisco 产品的 iOS 根据用户不同的功能需求,有多种不同的版本和特性,网络管理员必须根据自己的实际情况决定运行哪种版本的 iOS。为了方便网络管理员的操作,Cisco iOS 在不同的路由器上都配备了相同的用户接口。这使得在配置不同型号路由器时,网络管理员可以使用相同的命令。与微软公司早期的计算机操作系统 DOS 类似,iOS 是通过基于文本的命令行界面(Command Line Interface,CLI)来让网络管理员进行配置和管理的。使用命令行配置方式的优点主要是:在设备配置时提供了最大的灵活性,同时还可以使用一些脚本语言进行批量处理,这些优点是图形界面不具有的。由于 Cisco 在电信和企业级市场占有较高的份额,因此 Cisco 的 CLI 命令体系也被其他众多网络设备生产商模仿。本书也着重讲解 Cisco 的 CLI 命令。

2) JUNOS

瞻博(Juniper)公司的路由器使用的操作系统称为 JUNOS,是基于 UNIX FreeBSD 内核开发的高性能模块化路由器操作系统。JUNOS 针对传统路由器软件架构作了多项改进,简化了整个网络的部署、配置和恢复。例如,提交确认(Commit Confirm)功能使得在对远程设备进行配置发生意外断开(或会话终止)而系统又没有收到确认改动通知时,系统可以回到此前的配置状态;又如回滚(Rollback)功能,假如激活的配置导致运营性能劣化,JUNOS CLI 提供了 Rollback(回滚)命令,可以退回 50 步,即快速地恢复到此前的 50 个配置状态之一。与传统路由器撤销单个命令相比,使用回滚功能可以更快、更容易地恢复之前的配置。

3) VRP

中国华三通信技术有限公司(简称 H3C)是一家实力雄厚的路由器研发和生产厂商,主要提供 IT 基础架构产品及方案的研究、开发、生产、销售及服务。目前,华三通信在中国设有 38 个分支机构,公司员工约有 5000 人,其中研发人员占 55%。

在路由器领域,华三公司拥有完全自主知识产权的通用路由平台(Versatile Routing Platform,VRP),采用分布式的组件化灵活架构,有效地将 MPLS、QoS、流量工程、组播 VPN、可管理等诸多技术完美融合,结合创新的全分布式 NP/多核架构体系,使得 H3C SR 系列路由器实现了业务灵活性和高性能硬件转发的有机结合。

华三的 VRP 的设计思想与 Cisco 的 iOS 相似,但是华三的 CLI 命令与 Cisco 的 CLI 命

令并不一样。例如，Cisco 使用 show 命令显示信息，而华三则使用 display 命令显示信息，但是，实现相同功能的华三的配置命令一般都与 Cisco 的配置命令存在一一对应的关系。

3. 配置文件

配置文件是由网络管理员创建的文本文件。在每次路由器启动过程的最后阶段，路由器操作系统都会尝试加载配置文件。如果存在配置文件，路由器操作系统就会逐条执行配置文件中的命令，例如配置每个接口的 IP 地址和子网掩码、配置路由协议等。这样，当路由器断电或者重新启动时，网络管理员就不必对路由器中的各种参数重新进行配置，从而可以大大提高工作效率。

配置文件中所有的命令语句都是以文本格式保存的，其具体内容可以在路由器本地的控制台终端或远程的虚拟终端上显示、修改或删除，我们也可以通过简单文件传输协议(Trivial File Transfer Protocol，TFTP)将配置好的配置文件从路由器上传到服务器中，以便进行备份；反之，也可以通过 TFTP 将配置文件从服务器复制到路由器。

一般来说，在路由器中有以下两种类型的配置文件：

1）启动配置文件

启动配置文件也称为备份配置文件。在 Cisco 路由器中，启动配置文件保存在 NVRAM 中，并且在路由器每次初始化时，会自动加载到内存中变成运行配置文件。

2）运行配置文件

运行配置文件也称为活动配置文件，驻留在路由器的内存中。当通过路由器的命令行界面对路由器进行配置时，配置命令会被立即执行并自动添加到路由器的运行配置文件中。但是，这些新添加的配置命令并不会自动保存到 NVRAM 中。因此，每当网络管理员对路由器进行了重新配置或修改后，应该将当前的运行配置文件保存到 NVRAM 中，使之变成启动配置文件。

4. 实用管理程序

除了固化在路由器 ROM 中的 iOS 外，Cisco 公司还为其路由器产品提供了更直观的、图形化的、工作界面友好的配置和管理程序，如 SDM、CiscoWorks 等。

安全设备管理器(Security Device Manager，SDM)是 Cisco 公司提供的全新图形化路由器管理工具。这个管理工具利用 Web 界面、Java 技术和交互配置向导使得用户无须了解命令行接口(CLI)即可轻松地完成 iOS 路由器的状态监控、安全审计和功能配置，包括 QoS、Easy VPN Server、IPS、DHCP Server、动态路由协议等配置任务也可以利用 SDM 轻松而快捷地完成。使用 SDM 可以简化网络管理员的工作量和出错概率。使用 SDM 进行管理时，用户到路由器之间使用加密的 HTTP 连接及 SSHv2 协议，安全可靠。目前 Cisco 的路由器包括 8xx、17xx、18xx、26xx(XM)、28xx、36xx、37xx、38xx、72xx、73xx、75xx 和 12xxx 等系列产品都支持 SDM。

3.4　路由器的启动过程

路由器的启动过程如图 3-6 所示。

路由器的只读存储器(Read Only Memory，ROM)中包含 POST 加电自检(Power on Self Test)代码、BootStrap 引导代码、Mini iOS(简化版的 iOS，相当于 Windows 操作系统的

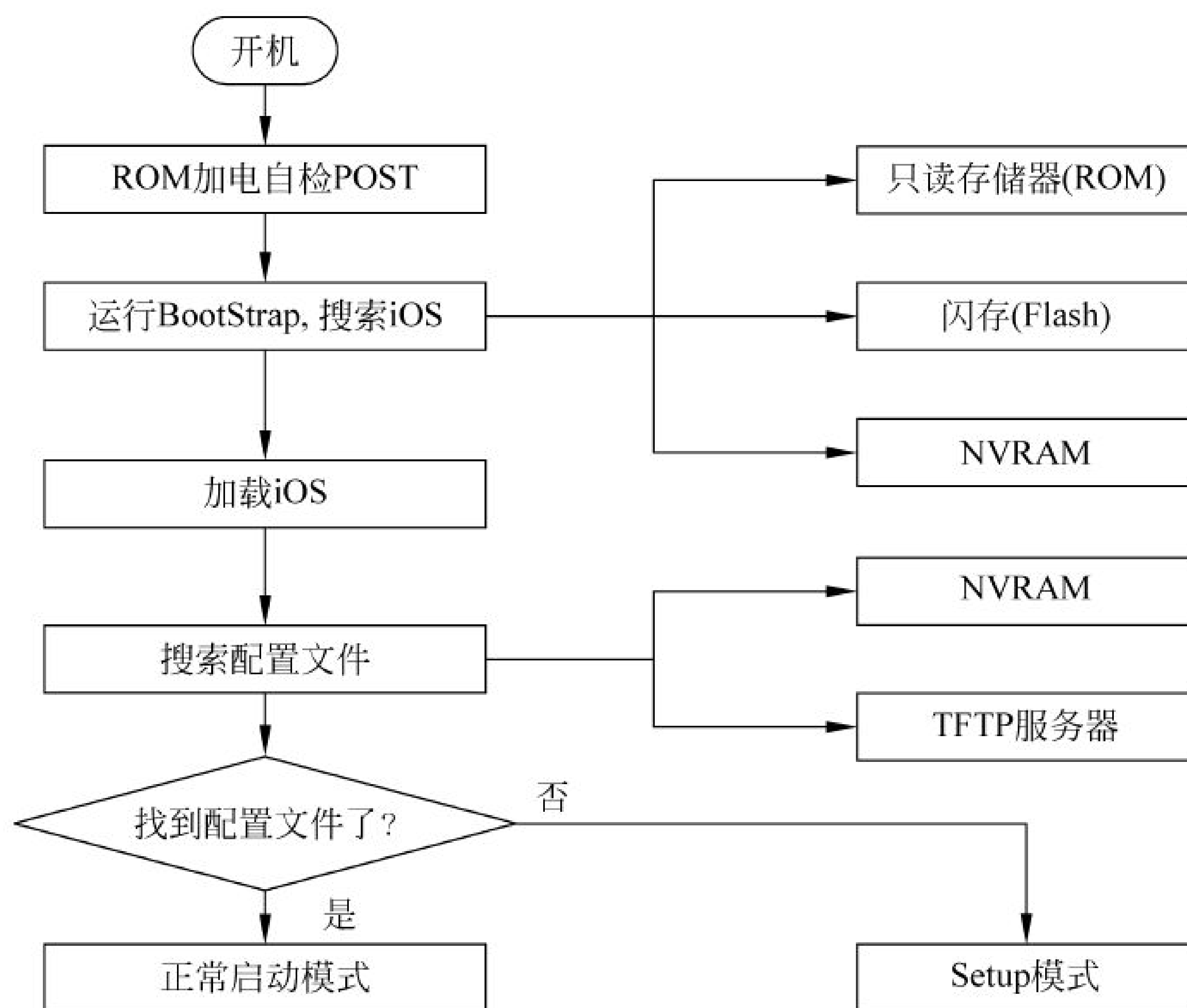


图 3-6 路由器的启动过程

安全模式)、ROM Monitor(相当于 Windows 操作系统的命令提示模式,主要用于灾难恢复)。而随机存取存储器(Random-Access Memory,RAM)中包含启动时加载的 iOS、各种路由协议进程、活动配置文件、缓冲区等。

路由器的 BOOT ROM 中存储着系统加载程序,系统启动时首先从 BOOT ROM 开始运行,由 BOOT ROM 负责加载整个操作系统。

NVRAM(非易失性存储器)使用 iOS 提供的相关命令对路由器进行配置,并将配置参数以配置文件的形式存放在 NVRAM 中,这样可便于在启动时加载到内存中。

(1) 系统硬件加电自检。运行 ROM 中的硬件检测程序,检测各组件能否正常工作。完成硬件检测后,开始软件初始化工作。

(2) 软件初始化过程。运行 ROM 中的 BootStrap 程序,进行初步引导工作。

(3) 寻找并载入 iOS 文件。

(4) iOS 加载完毕后,系统在 NVRAM 中搜索配置文件(Starup-Config),进行系统的配置。如果 NVRAM 中存在 Starup-Config 文件,则将该文件调入 RAM 中并逐条执行,否则系统进入 Setup 模式,进行路由器初始配置。

3.5 高端路由器

高端路由器是指在 Internet 骨干网核心使用的、性能优良、具有高密度高速端口和巨大交换容量的新一代路由器产品。按技术指标区分,通常将背板交换能力大于 40Gb 的路由器称为高端路由器,背板交换能力在 40Gb 以下的路由器称为中低端路由器。以市场占有率最大的 Cisco 公司为例,12000 系列为高端路由器,7500 以下系列路由器为中低端路由器。

高端 IPv6 路由器可提供高速交换式背板,无阻塞交换容量达到 64G/128G 或以上;提

供10G/2.5G POS、10GE、155M/622M POS等丰富的接口类型；符合IPv6相关的RFC(征求意见文档)标准规范；具备基于IPv4/ IPv6的线速包转发和包处理能力；模块化软件体系结构，多处理器分布式通信机制；分布式SNMP(简单网络管理协议)设计；组网灵活，体系支持MPLS(多协议标记转换)、RPR、MSR；高可靠性措施(如电源冗余配置)。

高端路由器在结构上一般设计成机柜形式，用背板进行信号转接，从而将十几块到几十块具有不同功能的插件卡联系在一起，来完成各种通信功能。针对这种机械结构，供电系统一般采用48V母线分布式供电结构，先将交流220V转换成直流48V，然后利用DC/DC转换器将48V转换成各插件卡所需的各种工作电压，如5V、3.3V、2.5V、1.8V和1.5V等。所有DC/DC转换器均与负载设计在一块印制板上或放置在距离负载板非常近的地方，再通过导线连接到负载板上。

专用多核网络处理器、专用转发芯片的研发和面世，使得高端路由器摆脱了以往的路由器靠纯软件转发的局限，向着高吞吐率、硬件快速转发等方向发展。高端的路由器设计成多板分布式+冗余备份的架构，使转发能力成倍增强，同时还大大提高了业务的稳定性。

目前，高端路由器大多采用专门的多核网络处理器作为CPU，如Cavium公司研发的Octeon系列处理器，主流的6000系列16～32个核，7000系列则多达64个核，并行处理能力大大加强，并且这类专用网络处理器在硬件上都对网络报文的解析、保序、转发等方面提供了专门的协处理器进行支持，优化并提高了系统的转发能力，也为软件研发者省去了不少麻烦。

Broadcom、Marvell等公司提供专门的转发芯片，通过VLAN、硬件路由等功能，在硬件上直接支持了对报文的高速转发，并且多片交换芯片之间可连接，最终形成一个大的交换矩阵网络。

CPU和交换芯片之间的数据通道可由10G高速接口相连，实现海量数据的传输；管理通道通过PCIe总线相连，传输控制信号。

随着宽带网络建设和行业信息化出现高潮，高端路由器正在逐步拓宽其应用范围，除Internet骨干网络等高端路由器传统应用领域外，高端路由器应用场合正向运营商城域网络、行业专网、企业网络、校园网等领域渗透。

随着国产厂商在高端路由器领域产品研发和市场开拓的力度不断加大，以华为、中兴、大唐等为代表的民族企业，正在迅速切入高端市场。作为国内民族通信产业优秀代表的华为，在高端路由器领域已经形成了极强的市场冲击力，成为Cisco在中国高端路由器市场无法忽视的竞争对手。华为NE系列高端路由器已在电信、移动等众多运营商市场得到大规模商用，打破了国外厂商一统高端路由器市场的格局。中兴ZXR系列高端路由器也已通过中国电信和中国联通设备选型及测试，并在上海、福建等地IP城域网中实现商用。此外，大唐、清华比威、烽火和巨龙等民族通信企业也在积极地推进其高端路由器的产业化进程。

3.6 路由表

路由器的主要工作就是为经过路由器的每个数据包寻找一条最佳的传输路径，并将数据包有效地传送到目的站点。由此可见，选择最佳路径的策略(即路由算法)是路由器的关键所在。为了完成这项工作，在路由器中保存每条传输路径的重要数据——路由表(Routing Table)，供路由选择时使用，表中包含的信息决定了数据转发的策略。换句话说，

路由表就像我们平时使用的地图一样，其中标识着各种路线。路由表中还保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。路由表可以是由系统管理员预先设置好的，也可以由系统动态修改，可以由路由器自动调整，也可以由主机控制。

根据路由器相关信息生成并维护路由表的方法来区分，路由可以分为直连（Direct）路由、静态（Static）路由和动态（Dynamic）路由。

用交叉线将两个路由器直接连接生成的路由称为直连路由。直连路由不需要配置。

系统管理员事先设置好固定的路由表称为静态路由表，一般是在系统安装时就根据网络的配置情况预先设定的，它不会随未来网络结构的改变而改变。

动态路由表是路由器根据网络系统的运行情况自动调整的路由表。路由器根据路由协议（Routing Protocol）提供的功能，自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

路由器通常依靠所建立及维护的路由表来决定如何转发。路由表能力是指路由表内所容纳路由表项数量的极限。由于 Internet 上执行 BGP 的路由器通常拥有数十万条路由表项，所以该项目也是路由器能力的重要体现。

所有的路由表一般都包含以下数据项：

第一，目的网络地址字段，是指向当前路由的目的字段。第二，子网掩码字段，用于指定网络前缀位数的子网掩码。第三，下一跳地址字段，当路由指向下一个路由器的接口时，下一跳字段的值为下一个路由接口的 IP 地址。第四，送出接口字段，用于指出当前 IP 数据包从路由器的哪个接口转发出去。

一个典型的路由表示例见表 3-1。

表 3-1 典型的路由表

目的网络地址	子网掩码	下一跳地址	送出接口
192.168.1.0	255.255.255.0	18.0.0.2	S0/0
10.0.0.0	255.0.0.0	2.0.0.1	E0/0
10.1.1.0	255.255.255.0	3.0.0.1	S0/1
0.0.0.0	0.0.0.0	4.0.0.1	E0/1

3.7 直连路由

直连路由是由链路层协议发现的，一般指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算获得，只要该接口处于活动状态（Active），路由器就会把通向该网段的路由信息填写到路由表中。直连路由无法使路由器获取与其不直接相连的路由信息。

这里，以图 3-7 所示的由 3 个路由器构成的网络环境为例来说明直连路由。

直连路由不需要任何配置命令，我们可以在特权模式（#）下用命令 show ip route 来查看路由器 2（即 Router2）的路由表，该命令执行的结果如图 3-8 所示。

在图 3-8 中，下面的以字母 C 带头的两条路由是直连路由，这表明路由器 Router2 通过这两条直连路由与另外两个路由器直接相连，直连的网络地址为 20.0.0.0/8 和 30.0.0.0/8。

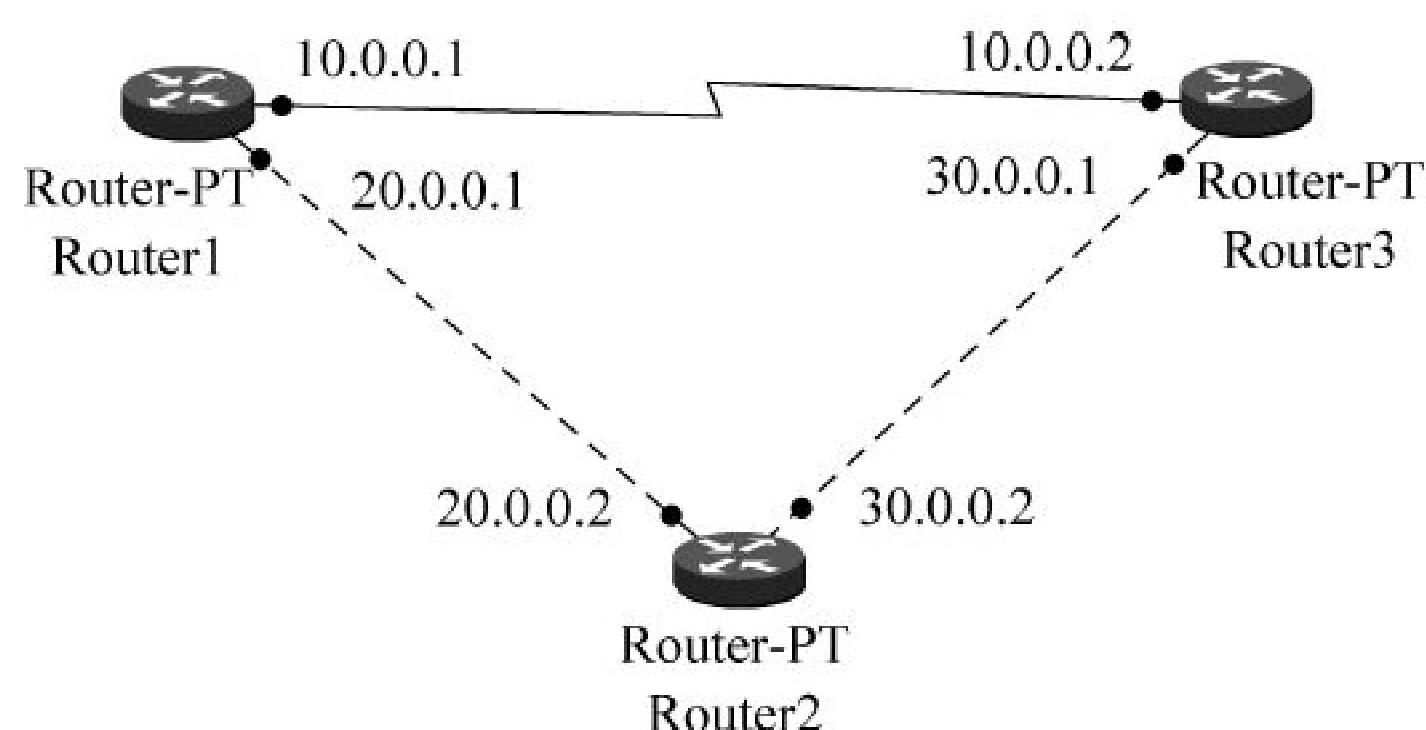


图 3-7　直连的 3 个路由器

```
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    10.0.0.0/8 [1/0] via 20.0.0.1
C    20.0.0.0/8 is directly connected, FastEthernet0/0
C    30.0.0.0/8 is directly connected, FastEthernet1/0
Router2#
```

图 3-8　直连路由实例

3.8　静态路由

静态路由的具体配置实例如图 3-9 所示。

```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
Router2(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    10.0.0.0/8 [1/0] via 20.0.0.1
C    20.0.0.0/8 is directly connected, FastEthernet0/0
C    30.0.0.0/8 is directly connected, FastEthernet1/0
Router2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 31/31/32 ms
```

图 3-9　静态路由的具体配置实例

静态路由是指由网络管理员或用户手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在默认情况下是私有的，不会传递给其他路由器。当然，网络管理员也可以通过对路由器进行设置使之成为共享的。

这里，我们仍用图 3-7 所示的网络环境为例，剖析静态路由配置的具体方法。

在图 3-9 中，第一条下画线所示的命令是在全局配置模式下，为路由器 2(Router2)配置一条静态路由，具体命令如下。

```
ip route 10.0.0.0 255.0.0.0 20.0.0.1
```

在图 3-9 中，用 show ip route 命令查看路由表，结果如第二条下画线所示：

```
S    10.0.0.0/8  [1/0]  via  20.0.0.1
```

以上这一行信息表明，这是一条静态路由(以字母 S 带头)，表明数据包要转发到网络地址 10.0.0.0/8，可以通过下一跳地址为 20.0.0.1 所指示的路径。

有关静态路由配置的方法，我们将在本书的第 5 章详细说明。

使用静态路由的另一个好处是网络安全保密性高。动态路由因为需要路由器之间频繁地交换各自的路由表，而对路由表的分析可以揭示网络的拓扑结构和网络地址等信息。因此，网络管理员出于安全方面的考虑，可以采用静态路由。静态路由不占用网络带宽，因为不会产生网络流量。

大型和复杂的网络环境通常不宜采用静态路由。一方面，网络管理员难以全面了解整个网络的拓扑结构；另一方面，当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围地调整，这个工作的难度和复杂程度非常高。当网络发生变化或网络发生故障时，不能重选路由，很可能使路由失败。

3.9 动态路由

本节仅简要地介绍动态路由协议的基本概念，不给出各种动态路由协议的具体配置实例。针对 RIP、OSPF 和 EIGRP 这 3 个典型的动态协议的工作原理，本书第 6～8 章将会对此作深入的剖析和阐述。

3.9.1 动态路由与静态路由的比较

动态路由是与静态路由相对的一个概念，指路由器能够根据路由器之间交换的特定路由信息自动地建立自己的路由表，并且能够根据链路和结点的变化适时地进行自动调整。当网络中结点或结点间的链路发生故障，或存在其他可用路由时，动态路由可以自行选择最佳的可用路由，并继续转发报文。

静态路由与动态路由的比较见表 3-2。

动态路由机制的运作依赖路由器的两个基本功能：路由器之间适时的路由信息交换和对路由表的维护。

表 3-2　静态路由与动态路由的比较

项　目	静 态 路 由	动 态 路 由
配置复杂性	随着网络规模的增加而越趋复杂	通常不受网络规模的限制
管理员所需知识	不需要额外的知识和技能	需要掌握高级的知识和技能
拓扑结构的变化	需要管理员参与	自动根据拓扑结构变化进行调整
可扩展性	适合于简单的网络拓扑结构	适合于简单的和复杂的网络拓扑结构
安全性	更安全	没有静态路由安全
资源占用情况	不需要额外的资源	占用 CPU、内存和链路带宽
可预测性	总是通过同一路径到达目标网络	根据当前网络拓扑结构决定路径

1. 路由器之间适时的路由信息交换

动态路由之所以能根据网络的情况自动计算路由、选择转发路径，是由于当网络发生变化时，路由器之间彼此交换的路由信息会告知对方网络的这种变化，通过信息扩散使所有路由器都能得知网络变化。

2. 对路由表的维护

路由器根据某种路由算法(不同的动态路由协议算法不同)把收集到的路由信息加工成路由表，供路由器在转发 IP 报文时查阅。

在网络发生变化时，收集到最新的路由信息后，路由算法重新计算，从而可以得到最新的路由表。

需要说明的是，路由器之间的路由信息交换在不同的路由协议中的过程和原则是不同的。交换路由信息的最终目的在于通过路由表找到一条转发 IP 报文的"最佳"路径。每种路由算法都有其衡量"最佳"的一套原则，大多是在综合多个特性的基础上进行计算，这些特性有：路径包含的路由器结点数(Hop Count)、网络传输费用(Cost)、带宽(Band Width)、延迟(Delay)、负载(Load)、可靠性(Reliability)和最大传输单元(Maximum Transmission Unit，MTU)。

3.9.2　静态路由的优缺点

1. 静态路由的优点

静态路由主要有以下优点。

(1) 占用的 CPU 处理时间较少。

(2) 便于网络管理员了解路由。

(3) 易于配置。

2. 静态路由的缺点

(1) 配置和维护耗费时间。

(2) 配置容易出错，特别是对于大型网络。

(3) 需要网络管理员维护变化的路由信息。

(4) 不能随着网络的增长而扩展，维护会越来越麻烦。

(5) 需要完全了解整个网络的情况才能进行配置。

3.9.3 动态路由的优缺点

1. 动态路由的优点

动态路由主要有以下优点。

(1) 增加或者删除网络时,网络管理员维护路由的工作量较少。

(2) 网络的拓扑结构发生变化时,协议可以自动调整。

(3) 配置不容易出错。

(4) 扩展性好,网络增长时不会出现问题。

2. 动态路由的缺点

(1) 工作时需要占用路由器的资源(CPU、内存和链路带宽)。

(2) 网络管理员需要掌握更多的网络知识才能进行配置、验证和故障排除工作。

3.9.4 动态路由协议的分类

常用的动态路由协议有 RIP、OSPF、IS-IS、BGP、IGRP 和 EIGRP 等。每种路由协议的工作方式、选路原则等都有所不同。

动态路由协议可以按照它们的特性分为不同的类别。

1. IGP 和 EGP

按照管理区域来分类,动态路由协议可以分为内部网关协议和外部网关协议两大类。

内部网关协议(Interior Gateway Protocol,IGP)是在一个自治网络内网关(主机和路由器)间交换路由信息的协议。路由信息能用于网间协议(IP)或者其他网络协议来说明路由传送是如何进行的。IGP 包括 RIP、OSPF、IS-IS、IGRP、EIGRP 等。

Internet 网被分成多个域或多个自治系统。一个域是一组主机和使用相同路由选择协议的路由器集合,并由单一机构管理。换言之,一个域可能是由一所大学或其他机构管理的互联网。IGP 在一个域中选择路由。外部网关协议(Exterior Gateway Protocol,EGP)为两个相邻的位于各自域边界上的路由器提供一种交换消息和信息的方法。

EGP 是自治区域(AS)之间使用的路由协议,最初于 1982 年由 BBN 技术公司的 EricC. Rosen 及 DavidL. Mills 提出。其最早在 RFC827 中描述,并于 1984 年在 RFC904 中被正式规范。EGP 是一种简单的(网络)可达性协议,其与现代的距离-矢量协议和路径-矢量协议不同,它仅适用于树状拓扑的网络。

EGP 是一个在自治系统网络中两个邻近的网关主机(每个网关主机都有它们自己的路由)间交换路由信息的协议。EGP 常常被用来在因特网的两个主机间交换路由表信息。路由表包括已知的路由器清单、它们能到达的地址以及与每个路由的路径相关的成本度量,以便选出最好的可用路径。每个路由器按照一定的时间间隔,通常在 120~480s 之间,给它的邻近路由器发送信息,然后邻近路由器就会将自己的完整路由表发回给它。EGP-2 是 EGP 的最新版本。

大部分的公司和机构将它们拥有的路由器组合成一个自治系统,自治系统的本地路由选择信息使用 RIP 或者 OSPF 等内部网关协议进行收集。而在这些自治系统中,通过为位于各自自治区域边界的两台相邻路由器提供交换路由选择信息的方法,选择一台或者多台路由器使用 EGP 与其他自治区域通信。EGP 路由器只向其自治区域边界上的路由器转发

路由选择表信息，来获得对方自治系统的路由信息，从而为 IP 数据报选择最佳路由。因此，EGP 应具有以下 3 个基本功能：

1）支持邻站获取机制

即允许一个路由器请求另一个路由器同意交换可达路由信息。

2）持续测试其 EGP 邻站是否有响应

EGP 应能够持续测试邻站是否有响应。

3）周期性地传送路由更新

EGP 邻站之间能够周期性地传送路由更新报文，交换网络可达路由信息。

2. 距离矢量和链路状态路由协议

IGP 可以分为距离矢量路由协议和链路状态路由协议两大类。

距离矢量路由协议（Distance Vector routing protocol，DV）是为小型网络环境设计的。在大型网络环境下，这类协议在学习路由及保持路由将产生较大的流量，占用过多的带宽。如果在 90s 内没有收到相邻站点发送的路由选择表更新，它才认为相邻站点不可达。

每隔 30s，距离矢量路由协议就会向相邻站点发送整个路由表，使相邻站点的路由表得到更新。这样，它就能从相邻的站点（直接相连的或其他方式连接的）收集整个网络的路由表，以便进行路由选择。距离矢量路由协议使用跳数作为度量值，来计算到达目的地要经过的路由器数。

链路状态路由协议（Link State Routing Protocol，LSRP）又称为最短路径优先（Shortest Path First，SPF）协议，它是基于 Edsger Dijkstra 的最短路径优先（SPF）算法。

链路状态路由协议比距离矢量路由协议复杂得多，但基本功能和配置却很简单，甚至算法也容易理解。路由器的链路状态的信息称为链路状态，包括接口的 IP 地址和子网掩码、网络类型（如以太网链路或串行点对点链路）、该链路的开销、该链路上的所有的相邻路由器。

链路状态路由协议是层次式的，网络中的路由器并不向邻居传递路由表，而是通告给邻居一些链路状态。与距离矢量路由协议相比，链路状态协议对路由的计算方法有本质的差别。距离矢量协议是平面式的，所有的路由学习完全依靠邻居，交换的是路由表。链路状态协议只是通告给邻居一些链路状态。运行该路由协议的路由器不是简单地从相邻的路由器学习路由，而是把路由器分成区域，收集区域的所有的路由器的链路状态信息，根据状态信息生成网络拓扑结构，每个路由器再根据拓扑结构计算出路由。

3. 有类和无类路由协议

有类的路由协议只会传送网络前缀（网络地址），但是不会包含子网掩码。当它传送更新时，它首先检查直接连接的网络是否和发送更新的网络属于同一个大一点的子网，如果是，那么它会继续检查它们的子网掩码是否相等，如果不相等，更新信息就会被丢弃，而不会被广播。

有类路由协议不支持可变长子网掩码（Variable Length Subnet Mask，VLSM），而无类路由协议传输网络前缀（网络地址）的同时也传输子网掩码，所以它支持 VLSM。

RIPv2、EIGRP、OSPF 和 BGP 等是一些比较新的无类路由选择协议，它们在路由更新过程中，会将子网掩码与路径一起广播出去，这时子网掩码也称为前缀屏蔽或前缀。例如，如果 C 类 IP 地址 192.168.1.0 的子网掩码为 255.255.255.0，则可标识为 192.168.1.0/24。

由于无类路由选择协议在路由器之间同时传送网络前缀和子网掩码，因而没有必要判断地址类型和默认掩码。

3.10 管理距离

不管是静态路由，还是动态路由，都要负责选择到达目的地网络的最佳路径，由于有可能某一台路由器上同时配置了几条路由（既配置了静态路由，又配置了动态路由，或者同时启用了几种动态路由协议），则到达同一目的地，网络就会有不同路由机制得到的多条不同的路径，因此就需要有一种方法，在这些路由中做出选择。选择最佳路由的示例如图 3-10 所示。

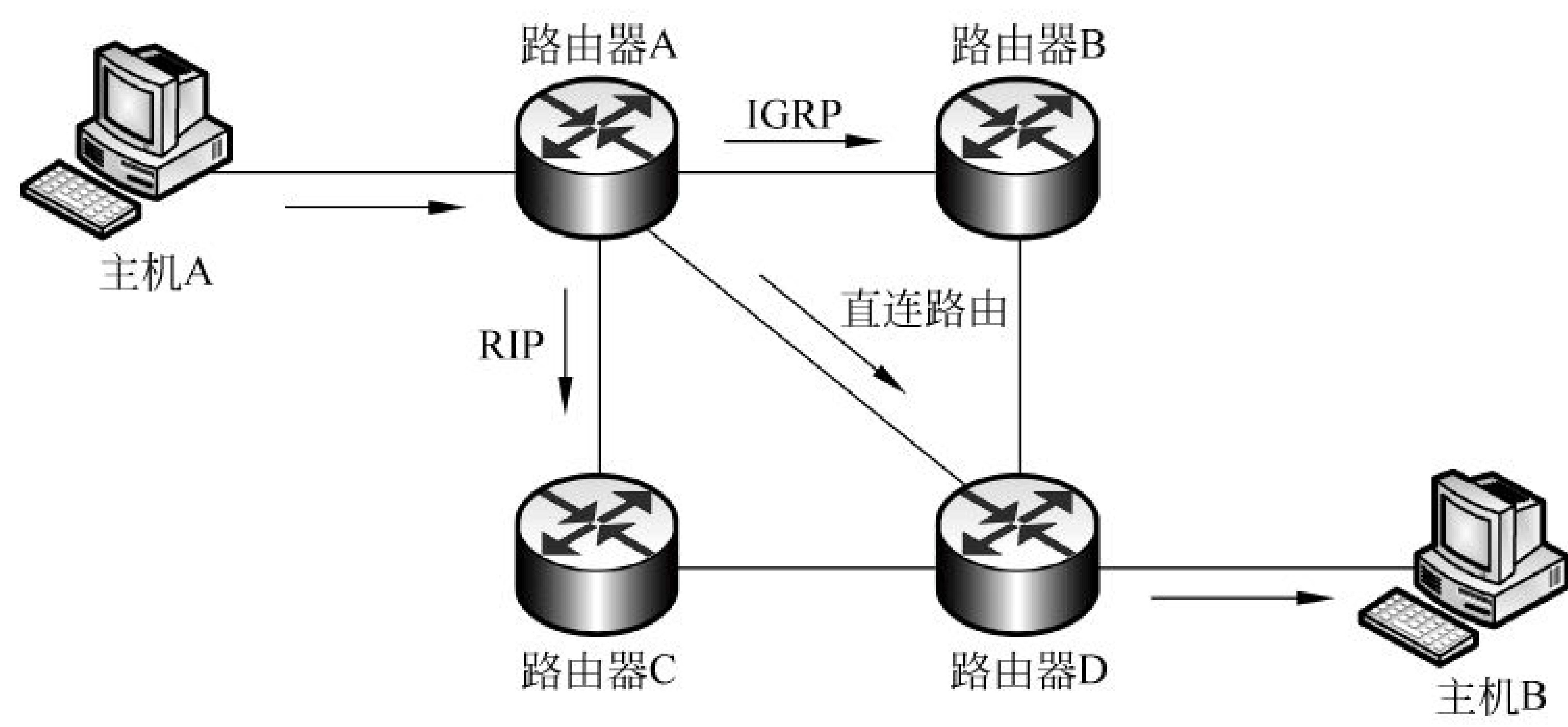


图 3-10 选择最佳路由的示例

在图 3-10 中，路由器配置了 3 种路由机制：直连路由、动态路由 RIP 和动态路由 IGRP。每种路由机制都根据自己的方法判断出从主机 A 到达主机 B 的最佳路径（其中，直连路由是自动生成的）。

直连路由：路由器 A→路由器 D。

动态路由 RIP：路由器 A→路由器 C→路由器 D。

动态路由 IGRP：路由器 A→路由器 B→路由器 D。

那么，实际上数据包究竟会怎样传输呢？

这就要涉及管理距离的概念。管理距离用于标识 IP 路由信息的可靠程度，即从这些路由机制中选择一种来使用，其他没有选中的路由机制也会正常工作，但不会被采用，直到被选中的路由机制失效。管理距离是一个 0～255 的整数，某个路由机制的管理距离越小，就认为这种路由机制越好，也越容易被采用。

默认的管理距离的分配原则如下：

（1）直接相连的路由条目管理距离最低，最容易被采用。

（2）静态路由的管理距离低于动态路由的管理距离。

（3）动态路由中，路由算法较精确的路由协议的管理距离低于路由算法较简单的路由协议的管理距离，因为算法越精确，找到的最佳路径就越准确。

表 3-3 给出了默认情况下的各种常用路由机制的管理距离。

表 3-3　默认情况下的各种常用路由机制的管理距离

路 由 机 制	默认管理距离
直连路由	0
静态路由	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
不知道的/不可信的	255(不会用来传输)

从表 3-3 中可以看出,管理距离能够保证当存在多个路由机制时,优先采用最合适的一种机制进行路由。

当然,网络管理员也可以人为地修改管理距离的值,来满足不同的网络需求。

3.11　本章总结

路由器(Router)是连接国际互联网中各个局域网、广域网的设备,它会根据信道的实际情况自动选择和设定路由,以最佳的路径按前后顺序发送数据包。路由器是互联网络的枢纽,就像“交通警察”一样管理着网络。

路由和交换机之间的主要区别就是交换机发生在 OSI 参考模型第二层(数据链路层),而路由发生在 OSI 参考模型的第三层,即网络层。这一区别决定了路由和交换机在移动信息的过程中须使用不同的控制信息,所以说两者实现各自功能的方式是不同的。

和其他计算机产品一样,路由器也是由硬件和软件组成的。路由器硬件包括中央处理器(CPU)、只读存储器(ROM)、随机存取存储器(RAM)、闪存(Flash)、非易失性存储器(NVRAM)、控制端口(Console)和辅助控制端口(AUX)、以太网接口、串行接口、扩展接口等;而路由器的主要软件是 iOS。但是,路由器硬件一般不包含硬盘。

路由器并没有自己专用的键盘、鼠标与显示器等输入/输出设备,因此,为了便于对路由器进行初始化配置和管理,路由器通常提供两个用于管理的接口:控制端口(Console)和辅助端口(AUX)。

路由器的只读存储器(Read Only Memory,ROM)中包含加电自检(Power on Self Test,POST)代码、BootStrap 引导代码、Mini iOS(简化版的 iOS 相当于 Windows 系统的安全模式)、ROM Monitor(相当于 Windows 的命令提示模式,主要用于灾难恢复)随机存取存储器(Random-Access Memory,RAM)包含启动时加载的 iOS、各种路由协议进程、活动配置文件、缓冲区等。

路由器的 BOOT ROM 中存储着系统加载程序,系统上电时首先从 BOOT ROM 开始运行,由 BOOT ROM 负责加载整个操作系统。

NVRAM(非易失性存储器)使用 iOS 提供的相关命令对路由器进行配置,并将配置参数以配置文件的形式存放在 NVRAM 中,这样可便于在启动时加载到内存中。

与其他计算机系统一样,软件也是路由器不可缺少的重要组成部分。路由器软件主要包括自举程序、路由器操作系统、配置文件和实用管理程序等。

高端路由器是指在 Internet 骨干网核心使用的、性能优良、具有高密度高速端口和巨大交换容量的新一代路由器产品。按技术指标区分，通常将背板交换能力大于 40Gb 的路由器称为高端路由器，背板交换能力在 40Gb 以下的路由器称为中低端路由器。

在路由器中保存着各种传输路径的相关数据——路由表(Routing Table)，供路由选择时使用，表中包含的信息决定了数据转发的策略。换句话说，路由表就像我们平时使用的地图一样，其中标识着各种路线，路由表中保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。

根据路由器的相关信息、生成并维护路由表的方法区分，路由可以分为直连(Direct)路由、静态(Static)路由和动态(Dynamic)路由。

直连路由是由链路层协议发现的，一般指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算获得，只要该接口处于活动(Active)状态，路由器就会把通向该网段的路由信息填写到路由表中。直连路由无法使路由器获取与其不直接相连的路由信息。

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在默认情况下是私有的，不会传递给其他路由器。

动态路由是与静态路由相对的一个概念，指路由器能够根据路由器之间交换的特定路由信息自动建立自己的路由表，并且能够根据链路和结点的变化适时地自动调整。当网络中结点或结点间的链路发生故障，或存在其他可用路由时，动态路由可以自行选择最佳的可用路由，并继续转发报文。

常见的动态路由协议有 RIP、OSPF、IS-IS、BGP、IGRP/EIGRP 等。

按照管理区域分类，动态路由协议可以分为内部网关协议和外部网关协议两大类。

内部网关协议(Interior Gateway Protocol，IGP)可以分为距离矢量路由协议和链路状态路由协议两大类。

有类路由协议不支持可变长子网掩码(VLSM)，而无类路由协议在传输网络前缀(网络地址)的同时也会传输子网掩码，所以它支持 VLSM。

当到达同一目的地，网络有多条不同路由机制得到的多条不同的路径时，就需要用管理距离在这些路由中做出选择。管理距离是一个 0～255 的整数，某个路由机制的管理距离越小，就认为这种路由机制越好，也越容易被采用。

复习思考题

1. 什么是路由器？请简要说明路由器的工作原理。
2. 请画图说明路由器的硬件结构。路由器包含硬盘吗？
3. 路由器的硬件由哪些部分组成？每一部分的主要功能是什么？
4. 路由器有哪些典型的接口？对路由器进行配置时一般使用哪些接口？
5. 路由器的软件主要包括哪些程序？这些程序的主要功能是什么？
6. Cisco 公司的 iOS 与中国华三公司的 VRP 操作系统有何异同？
7. 启动配置文件和运行启动配置文件有什么区别？

8. 请画图说明路由器的启动过程。
9. 高端路由器有什么主要的技术特点?
10. 什么是路由表?路由表主要包含哪些数据项?
11. 通常用什么命令查看路由表?
12. 什么是直连路由?直连路由需要用什么命令来配置?
13. 什么是静态路由?静态路由需要用什么命令来配置?
14. 什么是动态路由?动态路由算法计算和衡量最佳路由的原则是什么?
15. 请列表说明静态路由与动态路由的区别。
16. 常见的动态路由协议包括哪些协议?
17. 内部网关协议与外部网关协议有什么区别?
18. 什么是距离矢量路由协议?
19. 什么是链路状态路由协议?
20. 什么是有类路由协议?
21. 什么是无类路由协议?
22. 管理距离的作用是什么?哪种路由机制的默认管理距离最小?

第 4 章 路由器的基本配置

CHAPTER 4

4.1 互联网操作系统

与其他计算机产品一样，路由器和交换机等网络设备也需要操作系统才能运行。我们不妨把路由器比作人，那么，路由器操作系统就像是人的大脑一样，统一地指挥着路由器硬件的每个组成部分，使它们能互相协调地工作。如果没有操作系统的指挥，路由器的硬件设备就像没有灵魂的植物人一样，无法正常运转。对于思科(Cisco)公司的路由器或交换机产品来说，iOS 就是这些网络互联设备专用的操作系统，称为互联网操作系统(Internet working Operating System，iOS)。它是 Cisco 公司的核心技术，应用于 Cisco 的大多数产品中。这些 Cisco 路由器或交换机产品，无论其种类和型号如何，都离不开 Cisco iOS 的统一管理。

iOS 文件本身的大小为几兆字节，存储在闪存中。由于闪存可以提供非易失性存储功能，因此在闪存中保存的内容不会在设备断电时丢失。尽管内容不会丢失，但在需要时可以更新或覆盖。也就是说，通过更新闪存中的内容，可以将 iOS 升级到最新版本或为其添加新功能。

iOS 能够经济地和高效地管理路由器或交换机，并随着网络技术的不断发展动态地升级，以适应硬件和软件技术的不断进步。iOS 在网络管理过程中具有如下特点。

(1) 提供网络协议和网络服务功能。

(2) 在设备间提供高速的数据交换。

(3) 提供安全控制访问。

(4) 提供与网络资源的可靠连接。

iOS 提供的功能是通过命令行界面(Command Line Interface，CLI)实现的，但这些功能取决于 iOS 的版本和网络设备的类型。

4.2 网络设备的配置方式

网络设备与各种控制终端的连接方式如图 4-1 所示。对网络设备的配置和管理，主要借助计算机来进行。一般来说，路由器的配置方式主要有以下 4 种。

1. 用超级终端程序在本地直接配置

这种配置方式是使用配置线来进行连接，配置线的一端接到路由器的控制端口

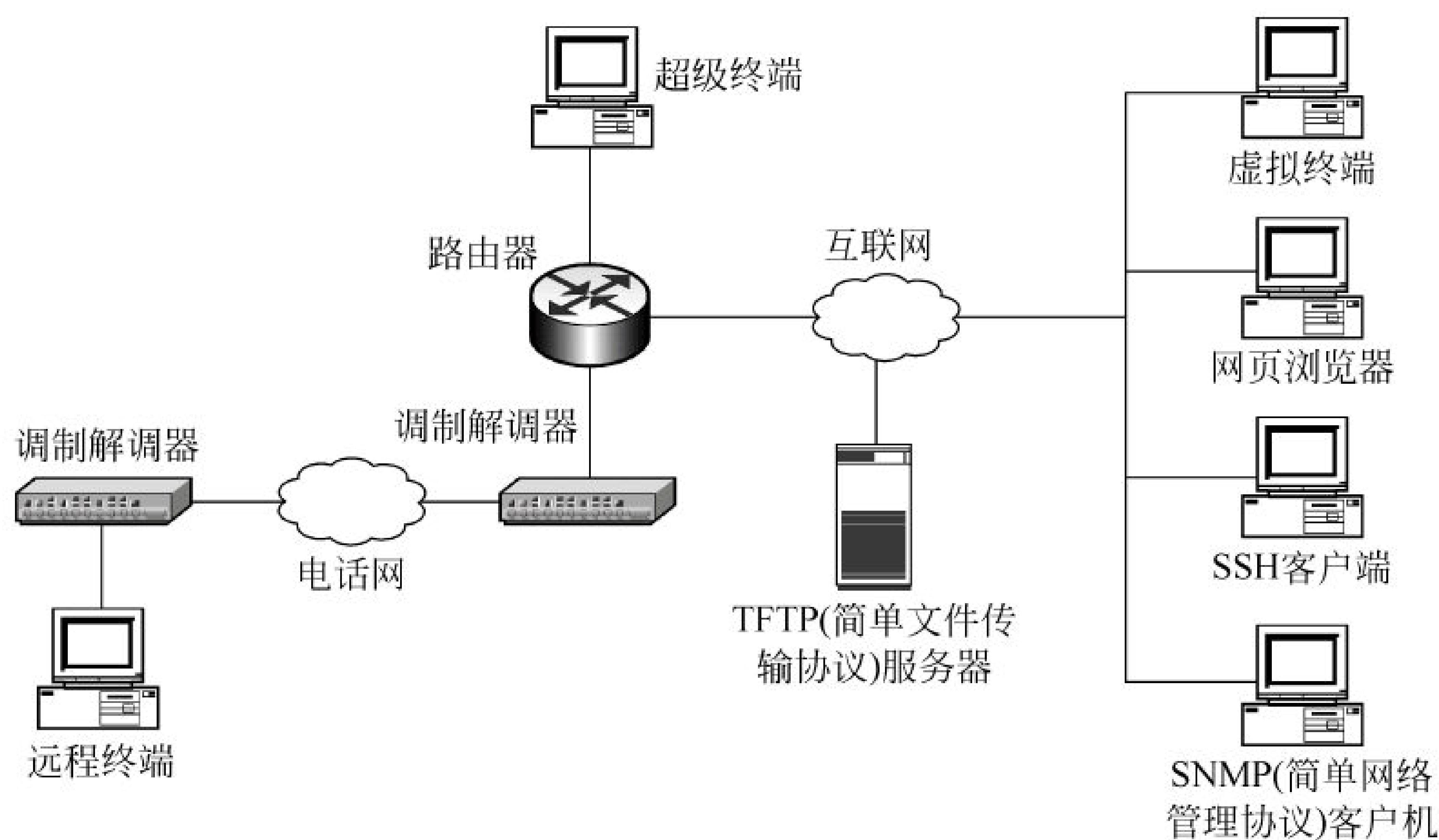


图 4-1　网络设备与各种控制终端的连接方式

(Console),配置线的另一端接到计算机(作为超级终端)的 RS-232 串行口。如果笔记本电脑没有 RS-232 串行口,则需要再配备一个 USB/RS-232 转接器。

这种通过控制端口对路由器进行访问的方式是最基本的配置方式,换句话说,对于刚出厂的思科路由器或交换机,第一次配置时,只能使用这种方式进行配置,而其他配置方式则需要经过授权后才能使用。特别地,对于刚出厂的 Cisco 路由器或交换机产品,从普通模式进入特权模式的原始密码一般都是 CISCO。

2. 通过调制解调器进行远程配置

这种配置方式是使用调制解调器(Modem)进行远程管理,将路由器的辅助端口(AUX)连接到调制解调器,接着通过电话网连接到远程的调制解调器,再接到远程终端。这样,网络管理员就可以通过远程网络拨号进行远程管理了。

3. 通过虚拟终端(Telnet)方式进行远程配置

这也是一种常用的远程配置方式。这是通过在互联网上某个用作虚拟终端的计算机上运行 Telnet 程序来实现远程配置的。进行远程登录前,必须在被控制的设备上配置 IP 地址,并确保该设备能在网络中工作。这种方式便于远程访问,但是由于 Telnet 采用明文方式传送报文,如果网络管理员的密码泄露或被黑客中途截获密码,就非常危险。

4. 通过 SSH 客户端方式进行远程配置

SSH(安全外壳协议)是目前较为可靠、专为远程登录和其他网络服务提供的安全性协议。使用 SSH 访问路由器时,使用数字证书认证 SSH 客户端和路由器之间的连接,并加密传输身份认证密码,可以有效防止欺骗、"中间人"和数据监听等网络攻击。SSH 协议有两个版本,即 SSH1 和 SSH2。这两个版本使用不同的协议实现,相互之间不兼容,SSH2 在功能和安全方面都比 SSH1 有所改进,因此得到广泛的应用。

除了以上介绍的 4 种常用的访问方式外,配置和管理路由器还可以通过 TFTP 服务器备份和恢复、通过 SNMP 客户机管理和通过网页浏览器的图形界面配置等方式。这些方式并不常用,这里,笔者就不详细介绍了。

4.3 配置超级终端

4.3.1 在 Windows XP 系统中配置超级终端

在路由器与计算机之间连接好配置线后，还需要在软件上进行配置。在 Windows XP 系统上启动超级终端程序的具体操作步骤如下：

(1) 启动“超级终端”程序。

在 Windows XP 系统上，依次选择“开始”→“所有程序”→“附件”→“通信”→“超级终端”选项，如图 4-2 所示。



图 4-2　在 Windows XP 上启动超级终端程序

(2) 打开“连接描述”对话框。

计算机的显示器会弹出“超级终端”对话框，接着会出现“连接描述”对话框。请在“连接描述”对话框中填入该连接的名称，用于标识该连接。例如，可以将连接的名称设置为“路由器”，如图 4-3 所示。



图 4-3　为连接命名

(3) 设置配置线所连接的串行口。

接着计算机会出现“连接到”对话框。在这一步骤中，请在“连接到”对话框中选择配置线所连接的计算机的串行口(RS-232 接口)。本例选择串行

口“COM1”，如图 4-4 所示。

（4）设置串行通信的参数。

接着，请在“COM1 属性”对话框中设置串行通信的参数。具体参数请按照图 4-5 所示的默认数据进行配置。请把“波特率”的值设置为 9600，“数据位”的值设置为 8，“奇偶校验”的值设置为“无”，“停止位”设置为 1，“流控制”设置为“无”。在这个步骤中，单击“还原为默认值”按钮，也可以把各个参数直接还原为默认值。



图 4-4　选择连接时使用的接口



图 4-5　设置串行通信的参数

（5）这样就可以进入超级终端的工作界面，如图 4-6 所示。

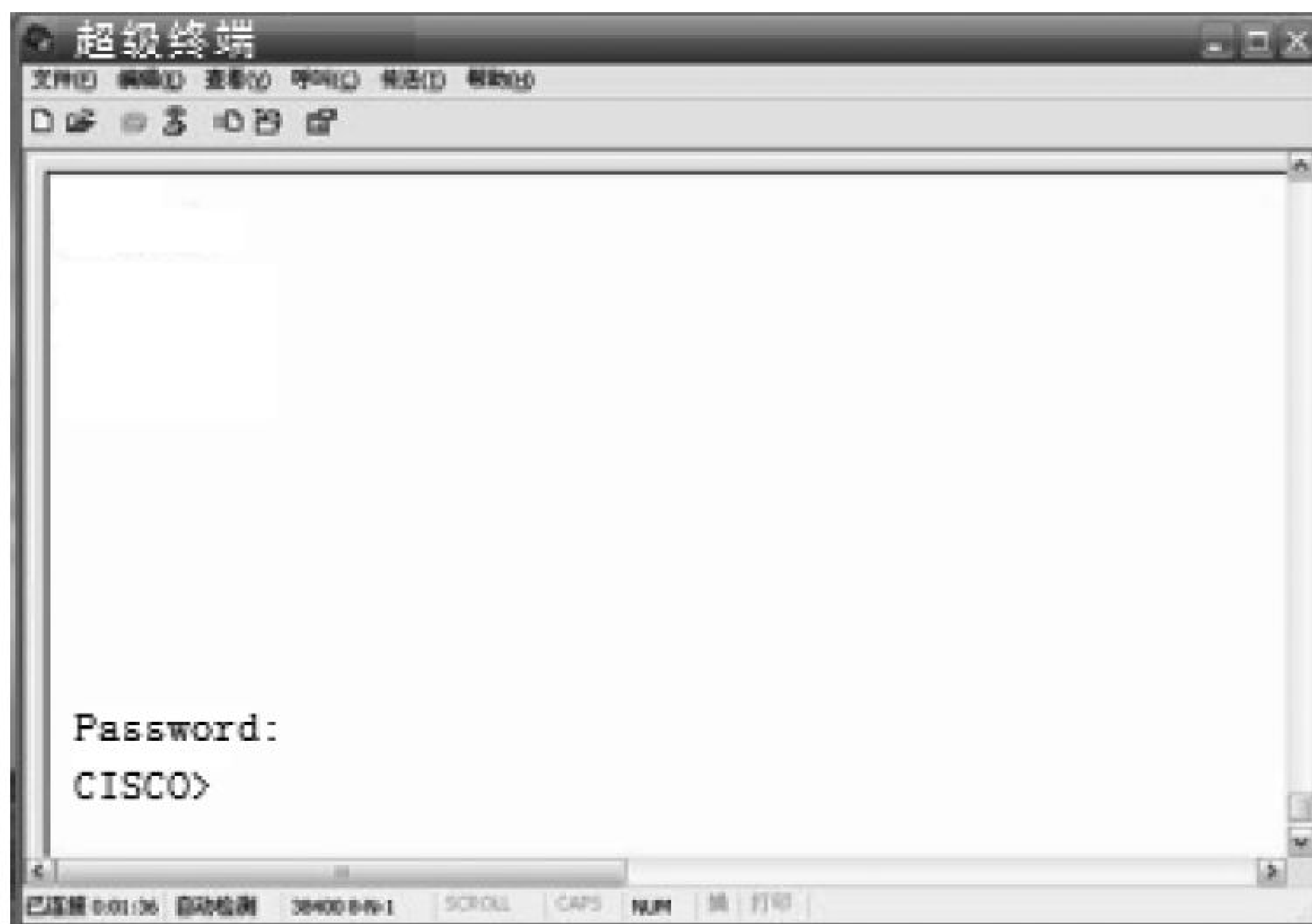


图 4-6　超级终端的工作界面

4.3.2　在 Windows 7 系统中配置超级终端

注意，在 Windows7 系统中并没有自带“超级终端”程序，我们可以从网上下载并安装专用的超级终端程序，如 hypertrm 程序、PUTTY 程序或者 SecureCRT 程序等。特别提醒：

要到信誉度高的软件网站下载,并用杀毒软件对下载的软件进行病毒检查。这些超级终端程序的配置方法与 Windows XP 系统中的配置方法相似,这里就不做详细介绍了。

4.4 路由器的配置向导

如上所述,路由器加电启动时,会查找启动配置文件(Startup-config),并将找到的启动配置文件加载到内存中运行。加载完成后,iOS 会询问网络管理员是否启用初始配置向导对话框。如果输入 y 或 yes,就可以进入路由器的配置向导。一般来说,我们不需要启用初始配置向导,所以请输入 n 或者 no 来回答。之后路由器会直接进入用户模式,如图 4-7 所示。

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of  ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T
1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n


Press RETURN to get started!
```

图 4-7　路由器的配置向导

4.5 路由器的工作模式

路由器的工作模式有多种,每种模式用于完成相应特定的任务。在每种模式下,具有各自不同的命令集。不同厂商的路由器的操作系统工作模式也不完全相同。Cisco 路由器 iOS 的工作界面是命令行接口(Command Line Interface,CLI),访问路由器时主要有两类操作:一类操作是执行某种命令,如显示系统的信息、设置路由器的日期和时间等立即要求执行的操作;另一类操作是对路由器进行配置,如配置接口 IP 地址、配置动态路由等,这类操作并不是立即执行,而是写入到内存的配置文件(Running-Config)中,并通过路由器的相应进程执行配置文件的内容。因此,思科将路由器的工作模式设计为两个部分:一部分是用于完成立即命令的"命令模式";另一部分是针对配置操作建立的"配置模式"。

基于安全考虑,思科将"命令模式"分成两个访问级别:一个是安全级别较低的"用户模式";另一个是安全级别较高的"特权模式"。从"特权模式"可转入"全局配置模式",而在"全局配置模式"上又可转入"接口配置模式""路由协议配置模式"和"线路配置模式"。

Cisco 路由器各种工作模式的提示符及其转换命令如图 4-8 所示。

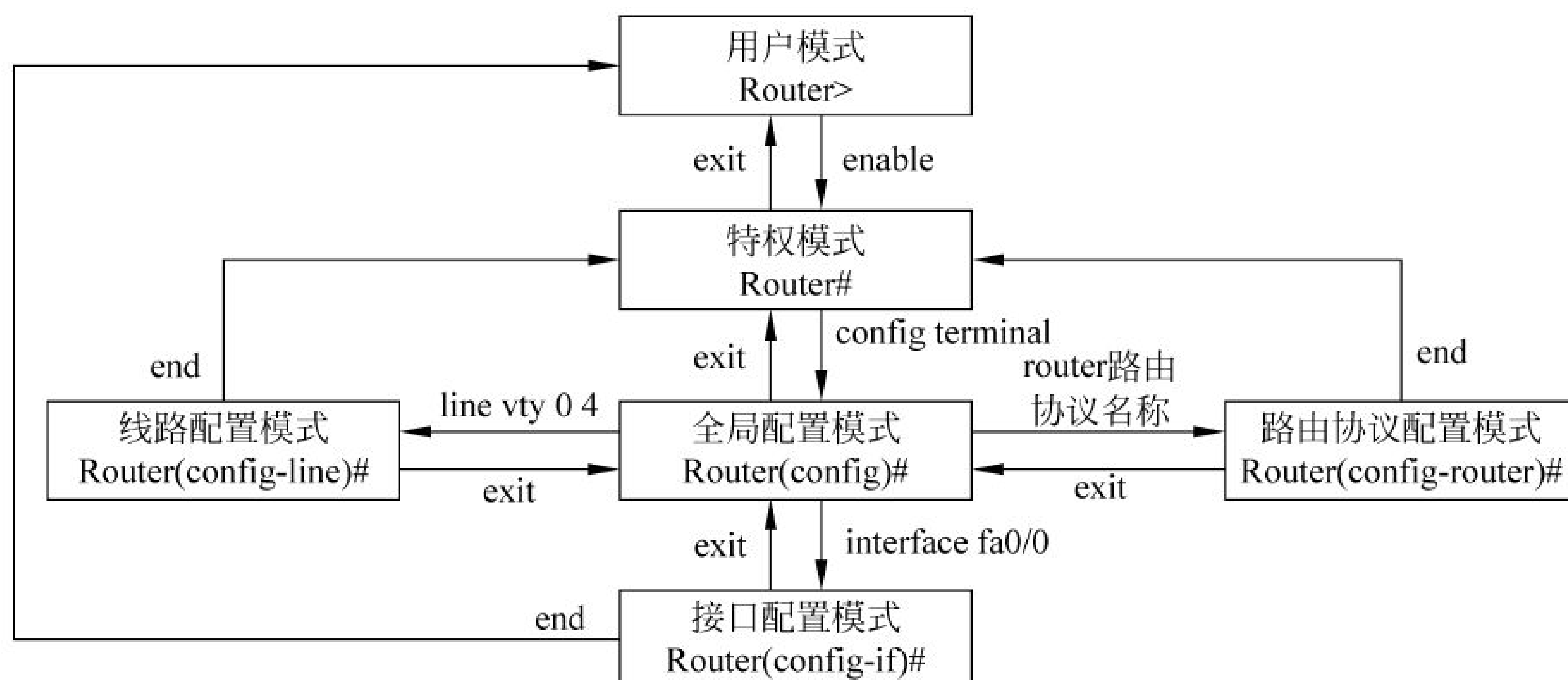


图 4-8　Cisco 路由器各种工作模式的提示符及其转换命令

1. 用户模式

用户模式(User EXEC)是路由器启动时的默认工作模式。用户模式的提示符为“路由器名称”+“>”,出现在每行命令的最前面,例如“Router >”。在用户模式下,路由器仅提供有限的访问权限,允许执行一些非修改性或破坏性的操作,如查看路由器的配置参数、测试网络的连通性等,但不能对路由器的配置参数进行修改。

2. 特权模式

从用户模式中可以通过 enable 命令和相应的密码进入到特权模式。特权模式的提示符为“路由器名称”+“#”,出现在每行命令的最前面,例如“Router #”。在特权模式(Privileged EXEC)下,网络管理员可以拥有比用户模式更多的权限。

在特权模式下,可以使用 exit 命令或 disable 命令返回用户模式。

3. 全局配置模式

从特权模式中可以通过 config terminal(可以简写为 conf t)命令切换到全局配置(Global Configuration)模式。全局配置模式的提示符为“路由器名称”+“(config)#”,出现在每行命令的最前面,例如“Router(config)#”。全局配置模式是路由器的更高级别的工作模式。网络管理员可以拥有修改路由器全局参数的权限,如设置时钟、修改路由器的名称、修改密码、配置路由协议等。

在全局配置模式下,可以使用 exit 命令返回特权模式。

4. 接口配置模式

接口配置(Interface Configuration)模式用于配置某个接口的参数。从全局配置模式中可以通过“interface 接口名称”命令切换到接口配置模式。接口配置模式的提示符为“路由器名称”+“(config-if)#”,出现在每行命令的最前面,如“Router(config-if)#”。

在接口配置模式下,可以使用 exit 命令返回全局配置模式,也可以使用 end 命令直接返回用户模式。

5. 路由协议配置模式

路由协议配置(Router Configuration)模式用于配置路由器的工作协议。从全局配置模式中可以通过“router 路由协议名称”命令切换到路由协议配置模式,例如 route RIP。

路由协议配置模式的提示符为“路由器名称”+“(config-router)#”,出现在每行命令的最前面,例如“Router(config-router)#”。

在路由协议配置模式下,可以使用 exit 命令返回全局配置模式。同样,也可以使用 end 命令直接返回特权模式。

6. 线路配置模式

线路配置(Line Configuration)模式用于配置某个接口的参数。从全局配置模式中可以通过“line vty 0 4”命令切换到线路配置模式。线路配置模式的提示符为“路由器名称”+“(config-line)#”,出现在每行命令的最前面,例如“Router(config-line)#”。

在线路配置模式下,可以使用 exit 命令返回全局配置模式。同样,也可以使用 end 命令直接返回特权模式。

7. 灾难恢复模式

灾难恢复(RXBOOT)模式用于路由器的灾难恢复。常见的灾难包括路由器密码丢失、操作系统软件被误删除后引起的路由器崩溃。在 Cisco 路由器电源开启 60s 内按下 Ctrl+Break 组合键就进入灾难恢复模式,在该模式下,路由器不能完成正常的路由与交换等网络功能,只能进行系统恢复和软件升级操作。

4.6 路由器的常用命令

在路由器的各种工作模式下,可以使用命令来实现路由器参数的查看、调试和配置工作。路由器的命令格式如下:

命令关键字 + 空格 + 一个或多个参数

对于不同厂商的路由器产品,实现同一功能的命令具体格式可能有所不同。例如,同样是查看路由器的路由表内容,思科路由器的命令格式是“show ip route”,而华三(H3C)路由器的命令格式则是“display ip routing-table”。为了便于初学者学习,本书仅介绍思科路由器的命令。思科路由器的常用命令如下。

1. 路由器的帮助命令

在用户模式下输入“?”命令,就可以得到相关命令的说明,如图 4-9 所示。

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  ipv6        ipv6
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Router>
```

图 4-9 “?”帮助命令返回用户模式各个命令的说明

为了实现各种复杂的功能，路由器操作系统提供了一个庞大的命令集。对于初学者来说，这些命令难以记忆。为此，路由器操作系统提供了路由器命令在线帮助功能，引导用户输入相关的命令。

实际上，无论当前在哪种工作模式下，网络管理员都可以输入"?"来请求帮助，iOS会给出当前工作模式下各个相关配置命令的格式及其功能说明。

2. 设置特权模式密码

基于安全性的要求，进入路由器的特权模式，需要输入密码。特权模式密码是从用户模式进入特权模式时使用的，其命令格式为：

enable password + 明文密码或 enable secret + 加密密码

注意：当使用命令 enable password＋明文密码配置密码时，路由器的安全性比较低。因为这种明文密码在内存配置文件中会以明文方式出现，当别有用心者使用"show running-config"或"show startup-config"命令时，就可以查看到用命令"enable password"所配置的"明文密码"，所以这样设置的"明文密码"形同虚设。

而当使用命令 enable secret ＋加密密码时，系统的安全性比较高。因为这种加密密码在内存配置文件中是以密文方式加以保护的，即使别人使用 show running-config 或 show startup-config 命令，也不能查看到用命令 enable secret 所设置的加密密码。

加密密码的优先级别比明文密码高，如果网络管理员同时配置了这两种密码，则当需要进入特权模式时，之前使用命令 enable password 配置的密码就会自动失效，必须输入用命令 enable secret 配置的加密密码。

3. 设置 Console 接口密码

配置 Console 接口密码的主要目的，是防止有机会进入网络中心的别有用心的人直接用配置线将计算机连接路由器的 Console 接口，进而恶意窥视，甚至篡改路由器的配置参数。

要设置 Console 接口密码，首先需要从全局配置模式下用命令"line console 0"进入 Console 线路配置模式；接着需要使用命令"password 密码"来设置登录密码；最后还要使用命令"login"要求端口实施登录验证。配置 Console 接口密码的具体实例如图 4-10 所示。在本例中，将 Console 接口密码设置为 supervisor。

```
CISCO>enable
CISCO#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CISCO(config)#line console 0
CISCO(config-line)#password supervisor
CISCO(config-line)#login
CISCO(config-line)#
```

图 4-10　配置 Console 接口密码的具体实例

4. 设置虚拟终端密码

虚拟终端(Telnet)密码是指网络管理员在远程计算机(即虚拟终端)上，通过虚拟终端方式登录到路由器时所需要输入的密码。如果路由器并没有配置虚拟终端密码，则用户不能通过远程方式访问路由器。配置虚拟终端密码的具体实例如图 4-11 所示。

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password john_marry
Router(config-line)#login
Router(config-line)#
```

图 4-11 配置虚拟终端密码的具体实例

在图 4-11 所示的配置虚拟终端密码的实例中，具体步骤说明如下：

(1) 在特权模式下用“config terminal”命令进入全局配置模式。

(2) 在全局配置模式下用“line vty 0 4”命令进入线路配置模式。

(3) 在线路配置模式下使用“password john_marry”命令将虚拟终端的密码设置为“john_marry”。

(4) 用“login”命令规定远程登录时必须验证密码。

(5) 此后，在虚拟终端上用“Telnet”+“路由器接口 IP 地址”命令，并输入相应的密码即可远程登录路由器了。

5. 修改路由器的名称

在全局配置模式下，可以用命令“hostname”+“路由器名称”修改路由器的名称。路由器的名称必须用字母开头，以字母或数字结尾。修改路由器的名称如图 4-12 所示。

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CISCO
CISCO(config)#
```

图 4-12 修改路由器的名称

如上所述，路由器的名称总是出现在 iOS 工作界面每行的命令的最前面。在图 4-12 所示的实例中，在全局配置模式下用命令“hostname CISCO”将路由器的名称从原来的“Router”修改为“ CISCO”。

6. 设置网络管理员无操作锁定时间

假如网络管理员由于某种原因，需要离开 Console 控制台一段不确定的时间。显然，如果离开时间过长，就给别有用心的破坏者有可乘之机。为了杜绝这类事件的发生，可以事先设置网络管理员无操作锁定时间。具体做法是在 Console 线路配置模式下使用命令“exit-timeout”进行配置，如图 4-13 所示。

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#exit-timeout 2 30
Router(config-line)#
```

图 4-13 设置无操作锁定时间

在图 4-13 中,命令"exit-timeout"的后面需要设置两个参数:第一个参数表示"分钟数";第二个参数表示"秒数"。在本例中,将锁定时间设置为 2 分 30 秒,意思是如果管理员在 2 分 30 秒的时间内没有对键盘输入任何命令,则路由器会自行锁定,回到用户模式,必须输入密码才能重新进入特权模式。

如果命令"exit-timeout"后面的这两个参数都设置为"0",则表示永不超时,即始终都不会锁定路由器。

7. 设置快速以太网接口的 IP 地址和子网掩码

路由器通常会提供两个 100M 的快速以太网接口,分别用"Fast ethernet 0/0"和"Fast ethernet 0/1"来编号。网络管理员可以用命令"interface 接口编号"和"ip address IP 地址 子网掩码"来设置快速以太网接口的 IP 地址和子网掩码,如图 4-14 所示。

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#
```

图 4-14 设置快速以太网接口的 IP 地址和子网掩码

在图 4-14 中,首先在全局配置模式下用命令"interface Fast Ethernet 0/0"指定需要配置的接口编号,接着用命令"ip address 10.0.0.1 255.0.0.0"指定接口 IP 地址为 10.0.0.1,子网掩码为 255.0.0.0,最后用命令"no shutdown"开启这个快速以太网接口。

8. 设置串行接口的 IP 地址和子网掩码

路由器通常也会提供若干个串行接口。串行接口一般用"Serial 0/0""Serial 1/0"和"Serial 2/0"等来编号。网络管理员同样可以用命令"interface 接口编号"和"ip address IP 地址 子网掩码"设置串行接口的 IP 地址和子网掩码,如图 4-15 所示。

```
Router(config)#interface Serial2/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#clock rate 9600
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down
Router(config-if)#
```

图 4-15 设置串行接口的 IP 地址和子网掩码

在直接互连的串行链路上,其中一端必须作为数据通信设备(DCE)设置时钟信号。时钟功能的启用和时钟频率的配置是使用命令"clock rate 时钟频率"来实现的。在本例中,将串行接口 Serial 2/0 的 IP 地址设置为 20.0.0.1,子网掩码设置为 255.0.0.0,时钟频率设置为 9600,并开启这个串行接口。

9. 查看路由器的参数

在对路由器进行配置或管理之前,或对路由器进行配置之后,都需要对路由器当前的工作状态参数进行检查。因此,所有的路由器都提供了用于查看路由器状态参数的命令。

(1) show version:查看版本号和引导信息。

(2) show running-config:查看正在运行的配置文件内容。

(3) show startup-config：查看启动配置文件的内容。

(4) show interface：查看接口信息。

(5) show ip interface brief：显示包括 IP 地址和接口状态在内的简要的接口配置信息。

(6) show ip route：查看路由表信息。

(7) show flash：查看闪存中的内容。

(8) show protocol：显示路由协议信息。

用命令"show running-config"可查看正在运行的配置文件内容，如图 4-16 所示。

```
Router#show running-config
Building configuration...

Current configuration : 520 bytes
!
version 12.2
no service password-encryption
!
hostname Router
!
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 --More--
```

图 4-16 查看正在运行的配置文件内容

图 4-16 返回的信息表明配置文件大小为 520B，路由器名字为 Router，SSH 访问方式的版本是第 1 版，快速以太网接口 FastEthernet 0/0 的 IP 地址为 10.0.0.1，子网掩码为 255.0.0.0。

命令"show running-config"返回的信息比较多，整个屏幕的空间都不能完全显示所有信息，所以 iOS 分开几页来显示命令"show running-config"返回的信息。在图 4-16 的显示页面中，按空格键即可继续显示下一页信息，如图 4-17 所示。

图 4-16 所示命令"show running-config"返回的第二页信息表明路由器除了快速以太网接口 FastEthernet 0/0 外，其余各个接口都未设置 IP 地址和子网掩码，并且都没有激活(shutdown)。

在图 4-17 的显示页面中，按空格键可以继续显示第三页的信息，如图 4-18 所示。图 4-18 中显示的信息表明当前路由器的控制台接口和虚拟终端接口都需要密码才能登录。

10. 测试网络连通性的命令(ping 命令)

ping 既是 Windows、UNIX 和 Linux 系统下的一个命令，也是路由器和交换机的基本命令。ping 也属于一个通信协议，是 TCP/IP 的一部分。利用 ping 命令可以检查网络是否连通，可以很好地帮助我们分析和判定网络故障。每条命令 ping 会执行 5 次连通性测试。命令的格式是：

```
ping + 空格 + IP 地址
```

```
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
ip classless
 --More--
```

图 4-17　查看正在运行的配置文件内容(续一)

```
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
ip classless
!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end


Router#
```

图 4-18　查看正在运行的配置文件内容(续二)

ping 命令用来检查网络是否通畅。利用网络上机器 IP 地址的唯一性,给目标 IP 地址发送一个数据包,再要求对方返回一个同样大小的数据包来确定两台网络机器是否连通,时延是多少。用 ping 测试网络的原则是由近及远,即首先测试本地接口 IP 地址,接着测试同一网段的接口 IP 地址,然后再测试更远的不同网段的 IP 地址。

这里,以图 4-19 所示的 3 个路由器构成的互联网络环境为例,来测试路由器的连通性。图 4-20 所示的是在路由器 2(Router2)中用 ping 命令测试路由器连通性的结果。

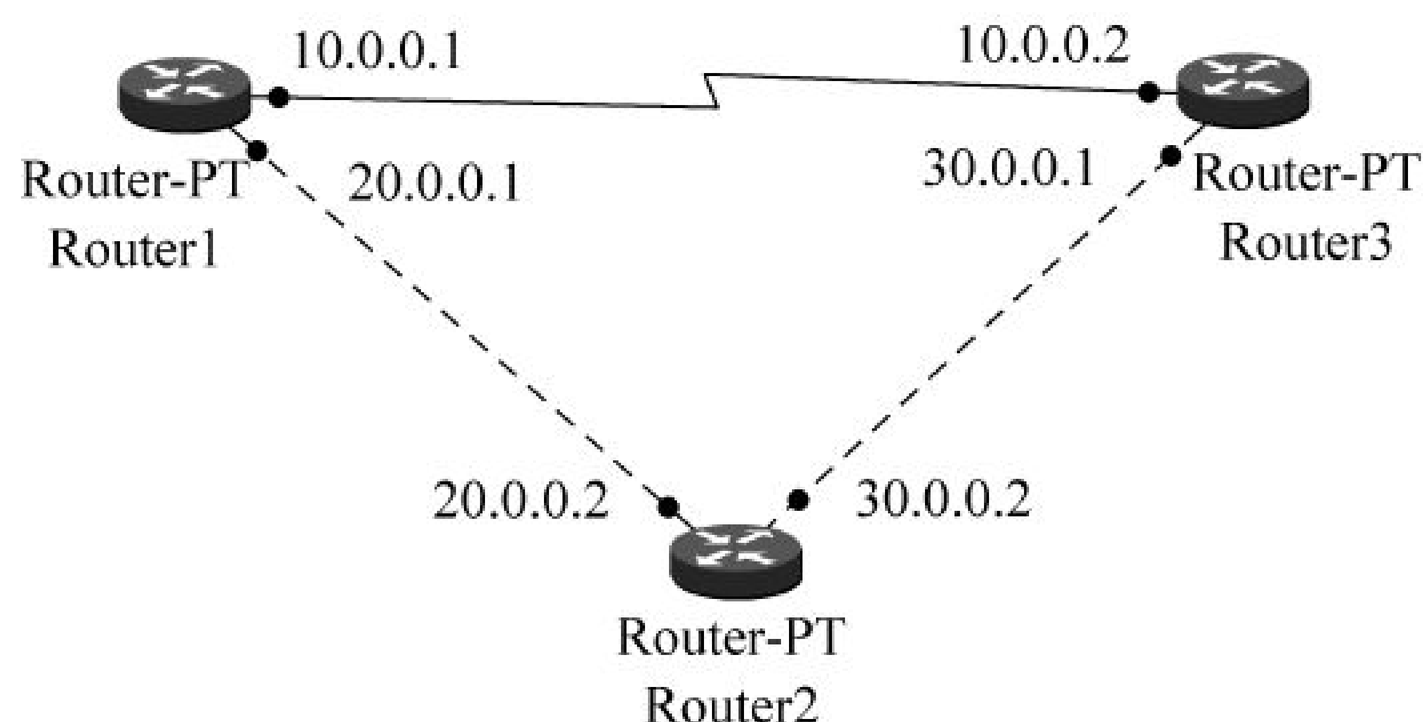


图 4-19　用于测试网络连通性的网络环境

```
Router2#ping 20.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/5 ms

Router2#ping 20.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 15/15/16 ms

Router2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms

Router2#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

图 4-20　网络连通性测试的结果

在图 4-20 中，第一条命令“ping 20.0.0.2”测试本地接口 IP 地址，结果是 5 个感叹号“!”；第二条命令“ping 20.0.0.1”测试直连的同一网段路由器 1(Router1)接口 IP 地址，结果是 1 个实心圆点“.”和 4 个感叹号“!”；第三条命令“ping 10.0.0.1”测试直连的同一网段路由器 1(Router1)接口 IP 地址，结果是 5 个感叹号“!”；第四条命令“ping 10.0.0.2”测试直连的同一网段路由器 1(Router1)接口 IP 地址，结果是 5 个实心圆点“.”。

在命令执行后出现的提示信息中，实心圆点“.”表示没有及时收到对方的回复数据包，说明网络不通；而感叹号“!”表示收到了对方的回复数据包，说明网络是连通的。

4.7　配置路由器 IP 地址的基本原则

路由器的每个端口都连接着一个具体的网络。为了让路由器正常工作，一般必须为路由器的端口设置 IP 地址。

路由器端口的 IP 地址的配置一般遵循以下 4 个原则：

（1）路由器的物理网络端口通常有一个 IP 地址。

（2）相邻路由器的相邻端口 IP 地址必须在同一个 IP 网段上。

（3）同一个路由器的不同端口的 IP 地址必须在不同的网段上。

（4）除了相邻路由器的相邻端口外，所有网络中路由器所连接的网段（即所有路由器的任何两个非相邻端口）都不能在同一个网段上。

相邻路由器的连接示例如图 4-21 所示。

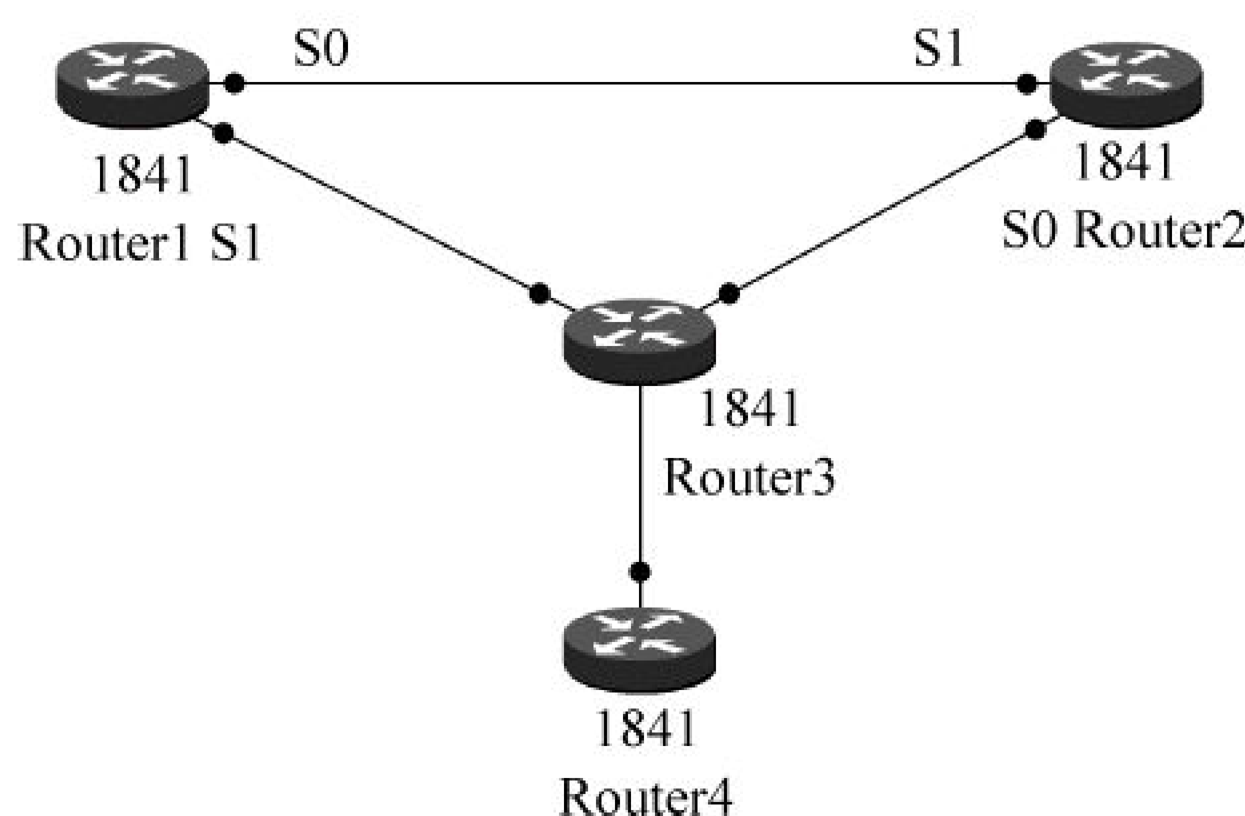


图 4-21　相邻路由器的连接示例

图 4-21 中有 4 个路由器，分别管理不同的网络段。对于路由器 Router1 和路由器 Router2 来说，它们互为相邻的路由器。其中，路由器 Router1 的 S0 端口与路由器 Router2 的 S1 端口为相邻端口。但是，路由器 Router1 的 S1 端口与路由器 Router2 的 S1 端口并不是相邻端口，路由器 Router1 与路由器 Router4 并不是相邻路由器。

4.8　iOS 的备份、恢复和升级

网络管理员日常工作中很重要的一个任务，就是保障思科 iOS 软件的安全性。而其中很重要的一个方法，就是 iOS 软件的备份与恢复。

1. iOS 软件备份与恢复的原则

在对思科路由器或者交换机的 iOS 软件进行升级之前，应当做好备份措施，即要先把原来存储在思科闪存中的 iOS 映像文件复制到 TFTP 服务器等网络设备上，以防止新的映像文件损坏或者烧毁而导致路由器不能正常运行。

这个原则非常重要，因为 iOS 映像文件至关重要，如果映像文件损坏或者烧毁而又没有备份，将导致 iOS 无法正常启动。iOS 软件升级，就是把 TFTP 上新的 iOS 映像文件复制到路由器的闪存中，如果闪存的容量不够大，就会覆盖掉原有的 iOS 映像文件。此时，如果新版本的 iOS 映像文件有问题，而以前的 iOS 映像文件因为已经被新版本覆盖掉，无法恢复，则就会导致路由器不能正常启动。若事先已经对旧版本的 iOS 映像文件进行了备份，则当出现了这种问题时，只需要对其进行简单的恢复操作即可。

2. iOS 软件备份与恢复前的准备工作

在对 iOS 软件进行备份或者恢复之前，网络管理员必须先做一些准备工作，以保障这些作业能够顺利进行。通常情况下，网络管理员需要验证 4 项任务。

(1) 要确保路由器等网络设备与TFTP服务器连接的正常性。

如果路由器不能够访问TFTP服务器,则备份或者恢复根本无法完成。这是因为路由器等网络设备与普通的主机毕竟有所不同。在路由器等网络设备上一般都没有足够的空间来保存路由器iOS的映像文件。也就是说,要对路由器的iOS软件进行备份,必须进行异地备份,这就必须要求路由器等网络设备能够访问网络上的TFTP服务器。

(2) 要确保TFTP服务器有足够的空间用来保存iOS软件备份。

虽然iOS映像文件一般不会像Windows操作系统那么庞大,在通常情况下,iOS映像文件不会超过100MB。不过,为了安全方面的需要,在对iOS软件进行备份之前,网络管理员还是需要确认一下,看用作保存备份文件的TFTP服务器是否有足够的空间可供使用。

(3) 需要验证所需要备份的iOS文件名与路径。

通常情况下,路由器和交换机等网络设备的iOS映像文件是存储在闪存中的。但是,在一些特殊的应用情况下,路由器也可以从远程TFTP服务器上运行iOS软件。所以,网络管理员在备份或者升级iOS软件前,需要事先确认一下当前需要备份或者升级的路由器,其运行的是哪一个位置上的iOS软件。

(4) 需要验证TFTP服务器的默认路径。

恢复iOS软件时需要验证其使用的iOS映像文件是否已经被保存在TFTP服务器的默认路径下。这项任务非常重要。因为在通常情况下,从TFTP服务器把iOS映像文件恢复到路由器的闪存中的时候,会把TFTP服务器默认路径下的iOS映像文件复制到路由器的闪存中。如果TFTP服务器下没有可用的iOS映像文件,则这个恢复工作就会以失败告终。TFTP服务器是局域网中的一台计算机,同时提供应用层接入方式,可以运行Web应用程序和实现客户端/服务器(C/S)模式或浏览器/服务器(B/S)模式的访问。

3. iOS的备份

iOS的备份实际上就是把路由器的iOS映像文件复制到一台TFTP服务器中。具体操作步骤如下:

(1) 安装TFTP服务器。

安装TFTP服务器的方法很简单,只要在某一台计算机上从网上下载、安装并运行一个名字为"tftpd32.exe"的TFTP服务器程序,就可以使这台计算机变成一台TFTP服务器。

(2) 连接TFTP服务器并配置IP地址。

用双绞线将计算机的以太网卡与路由器的Fast Ethernet 0/0接口连接起来,并为网卡和Fast Ethernet 0/0接口配置同一个网段的IP地址,如图4-22所示。

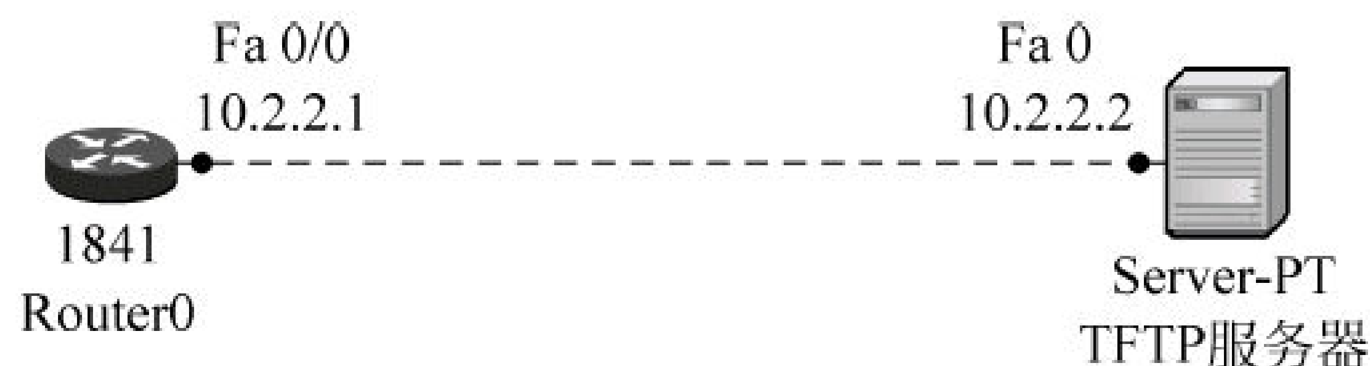


图4-22 连接TFTP服务器

(3) 用ping命令测试连通性。

在路由器的特权模式下执行命令"ping 10.2.2.2",测试与TFTP服务器的连通性,确认网络连接正常。

(4) 查看 iOS 的映像文件名。

在全局配置模式下输入命令“dir flash:”,这条命令返回当前路由器的以.bin 为后缀的 iOS 映像文件名。

(5) 执行 iOS 备份命令。

在路由器的特权模式下执行命令“copy flash: tftp:”,此时,路由器会首先要求输入 iOS 映像文件名,接着要求输入 TFTP 服务器的 IP 地址,最后会询问这个 iOS 映像文件在 TFTP 服务器上的文件名,此时,如果不打算修改文件名,那么直接按 Enter 键即可开始执行备份操作,整个备份过程可能需要几分钟时间。

(6) 确认备份成功。

最后一步,就是到扮演 TFTP 服务器的计算机相关的文件夹中,确认一下是否真的存在 iOS 映像文件。

4. iOS 的恢复

iOS 的恢复过程与备份过程正好相反,实际上就是把 TFTP 服务器中的 iOS 映像文件复制到路由器的闪存中。其连接与配置 IP 地址方法与备份时的配置方法完全相同,这里就不再重复了。

在恢复 iOS 映像文件时,只要首先在计算机中运行名字为“tftpd32.exe”的 TFTP 服务器程序,使这台计算机变成一台 TFTP 服务器;然后在路由器的特权模式下执行以下恢复命令“copy tftp: flash:”,并按相关的提示信息输入 IP 地址和映像文件名即可。

5. 升级 iOS

升级 iOS 实际上就是到思科的官方网站下载最新版本的 iOS 映像文件,并用与恢复 iOS 映像文件相似的方法复制 iOS 映像文件,就可以使路由器操作系统升级到最新的版本,从而改善路由器的性能。注意,下载的 iOS 映像文件必须与路由器的型号完全匹配,否则升级不当,有可能导致路由器瘫痪,所以请务必谨慎地进行升级操作。

4.9 本章总结

与其他计算机产品一样,路由器和交换机等网络设备也需要操作系统才能运行。我们不妨把路由器比作人,那么,路由器操作系统就像是人的大脑一样,统一地指挥着路由器的每个硬件,使之能互相协调地正常工作。如果没有操作系统的指挥,路由器的硬件设备就像植物人一样,无法正常运转。对于思科(Cisco)公司的路由器或交换机产品来说,iOS 就是这些网络互联设备专用的系统软件,称为互联网操作系统(Internet working Operating System,iOS)。

一般来说,路由器的配置方式主要有以下几种。

(1) 用超级终端程序在本地直接配置。

(2) 通过调制解调器进行远程配置。

(3) 通过虚拟终端(Telnet)方式进行远程配置。

(4) 通过 SSH 客户端方式进行远程配置。

在路由器与计算机之间连接好配置线后,还需要在软件上进行配置,即在 Windows XP 系统上启动超级终端程序。

注意，在 Windows 7 系统中并没有自带“超级终端”程序，我们可以从网上下载并安装专用的超级终端程序，如 hypertrm 程序、PUTTY 程序或者 SecureCRT 程序等。

路由器操作系统的工作模式有多种，每种模式用于完成相应特定的任务。在每种模式下，具有各自不同的命令集。

基于安全考虑，思科将“命令模式”分成两个访问级别：一个是安全级别较低的“用户模式”；另一个是安全级别较高的“特权模式”。而在“全局配置模式”上，又可以进入“接口配置模式”“路由协议配置模式”和“线路配置模式”。

在路由器工作模式下，使用命令来实现路由器的查看、调试和配置工作。路由器的命令格式如下：

```
命令关键字 + 空格 + 一个或多个参数
```

Cisco 路由器的常用命令如下。

（1）路由器的帮助命令。

（2）设置特权模式密码。

（3）设置 Console 接口密码。

（4）设置虚拟终端密码。

（5）修改路由器的名称。

（6）设置网络管理员无操作锁定时间。

（7）设置快速以太网接口的 IP 地址和子网掩码。

（8）设置串行接口的 IP 地址和子网掩码。

（9）查看路由器的参数。

（10）测试网络连通性的命令（ping 命令）。

网络管理员日常工作中很重要的一个任务，就是保障思科 iOS 软件的安全性。而其中很重要的一个方法，就是 iOS 软件的备份与恢复。

iOS 的备份实际上就是把路由器的 iOS 映像文件复制到一台 TFTP 服务器中。

iOS 的恢复过程与备份过程正好相反，实际上就是把 TFTP 服务器中的 iOS 映像文件复制到路由器的内存中。

升级 iOS 实际上就是到思科的官方网站下载最新版本的 iOS 映像文件，并用与恢复 iOS 映像文件相似的方法来复制 iOS 映像文件，就可以使路由器操作系统升级到最新的版本，从而改善路由器的性能。

复习思考题

1. 什么是 iOS?
2. iOS 具有什么特点?
3. 怎样用超级终端对路由器进行配置?
4. 怎样用调制解调器对路由器进行远程配置?
5. 怎样用虚拟终端对路由器进行配置?
6. 怎样用 SSH 客户端对路由器进行远程配置?

7. 在 Windows XP 系统中怎样配置“超级终端”?

8. 在 Windows 7 系统中怎样配置“超级终端”?

9. 怎样进入路由器的配置向导模式?

10. 什么是用户模式? 其提示符是什么?

11. 什么是特权模式? 其提示符是什么? 如何从用户模式进入特权模式?

12. 什么是全局配置模式? 其提示符是什么? 如何从特权模式进入全局配置模式?

13. 什么是接口模式? 其提示符是什么? 如何从全局配置模式进入接口模式?

14. 什么是路由器配置模式? 其提示符是什么? 如何从全局配置模式进入路由器配置模式?

15. 什么是线路配置模式? 其提示符是什么? 如何从全局配置模式进入线路配置模式?

16. 什么是灾难恢复模式? 如何进入灾难恢复模式?

17. 路由器的命令格式是什么?

18. 如何使用路由器的帮助命令?

19. 如何设置从用户模式进入特权模式的两种密码?

20. 如何设置控制台(Console)接口密码?

21. 如何设置虚拟终端密码?

22. 如何修改路由器的名称?

23. 如何设置网络管理员无操作锁定时间?

24. 如何设置快速以太网接口的 IP 地址和子网掩码?

25. 如何设置串行接口的 IP 地址和子网掩码?

26. 路由器的参数包括哪些命令? 这些命令的功能是什么?

27. 如何测试网络的连通性?

28. 在执行测试连通性命令返回的信息中,冒号“!”代表什么? 实心圆点“.”又代表什么?

29. 配置路由器 IP 地址的基本原则是什么?

30. 为什么要备份 iOS?

31. 在进行 iOS 软件备份与恢复操作之前,要做好哪些准备工作?

32. 如何备份 iOS?

33. 如何恢复 iOS?

34. 如何升级 iOS?

第 5 章 静 态 路 由

CHAPTER 5

路由协议是路由器软件中的重要组成部分。路由器为互联的网络之间选择最佳的通信路径都是通过这些路由协议来完成的。路由协议的作用还在于建立以及维护路由表。路由表用于对每个 IP 数据包选择输出端口或下一跳地址。

5.1 基本的 IPv4 静态路由配置

静态路由是在路由器中设置的固定的路由表,即由网络管理员指定的固定的传输路径。除非网络管理员干预,否则静态路由不会自动更改。所以,当网络的拓扑结构或链路的状态发生变化时,需要网络管理员手工修改路由表中的相关静态路由信息。默认情况下,静态路由信息是私有的,不会传递给其他路由器。

静态路由是一种特殊的路由,它由网络管理员手工配置而成。通过静态路由的配置可以建立一个互联的网络。但是,静态路由的缺点在于:当一个网络故障发生后,静态路由不会自动发生改变,因此需要网络管理员的介入。

当要指定数据包转发的路径时,需要配置静态路由。静态路由是由网络管理员手工配置的路由,这些路由明确指定了数据包从起点到目的地必须经过的路径。静态路由的特点如下:

(1) 它允许对路由的行为进行精确的控制。由于静态路由是手工配置的,网络管理员就可以通过静态路由来控制数据包在网络的流动。

(2) 静态路由减少了网络的流量。因为静态路由不需要路由器之间互相通信来学习路由,这一点在某些情况下是非常重要的。例如,使用按需要拨号路由(DDR)时,必须使用静态路由,因为如果使用动态路由,路由更新会导致不停地进行拨号连接。

(3) 静态路由是单向的。也就是说,如果希望实现双方的通信,必须在通信双方都配置静态路由。

(4) 简化配置。有时网络的拓扑结构很简单,路径是显而易见的。此时就没有必要配置动态路由来浪费带宽和路由器的资源了。

(5) 静态路由缺乏灵活性。静态路由虽然能对数据包路径进行精确控制,但是又限制了灵活性。因为它是静态配置的,不能根据网络的变化而灵活改变,因此当网络拓扑结构更新时,如链路故障,网络管理员就必须重新配置该路由。

静态路由通常不适合大型和复杂的网络环境,原因包括两个方面:一是网络管理员很

难做到对大型和复杂的网络进行全面了解；二是当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围的修改，修改的难度和复杂度非常高，如果配置错误，还有可能导致路由环路。

静态路由有 3 种典型的应用。

(1) 网络环境比较简单，网络管理员可以很清楚地了解其网络的拓扑结构。

(2) 由于安全原因，希望隐藏网络的一部分。

(3) 用于访问末节网络。

要配置 IPv4 静态路由，可以在全局配置模式下使用以下两条配置命令之一：

```
ip route 网络地址 子网掩码 下一跳地址
ip route 网络地址 子网掩码 送出接口名称
```

下面以图 5-1 所示的网络环境为例，介绍基本静态路由的配置方法。

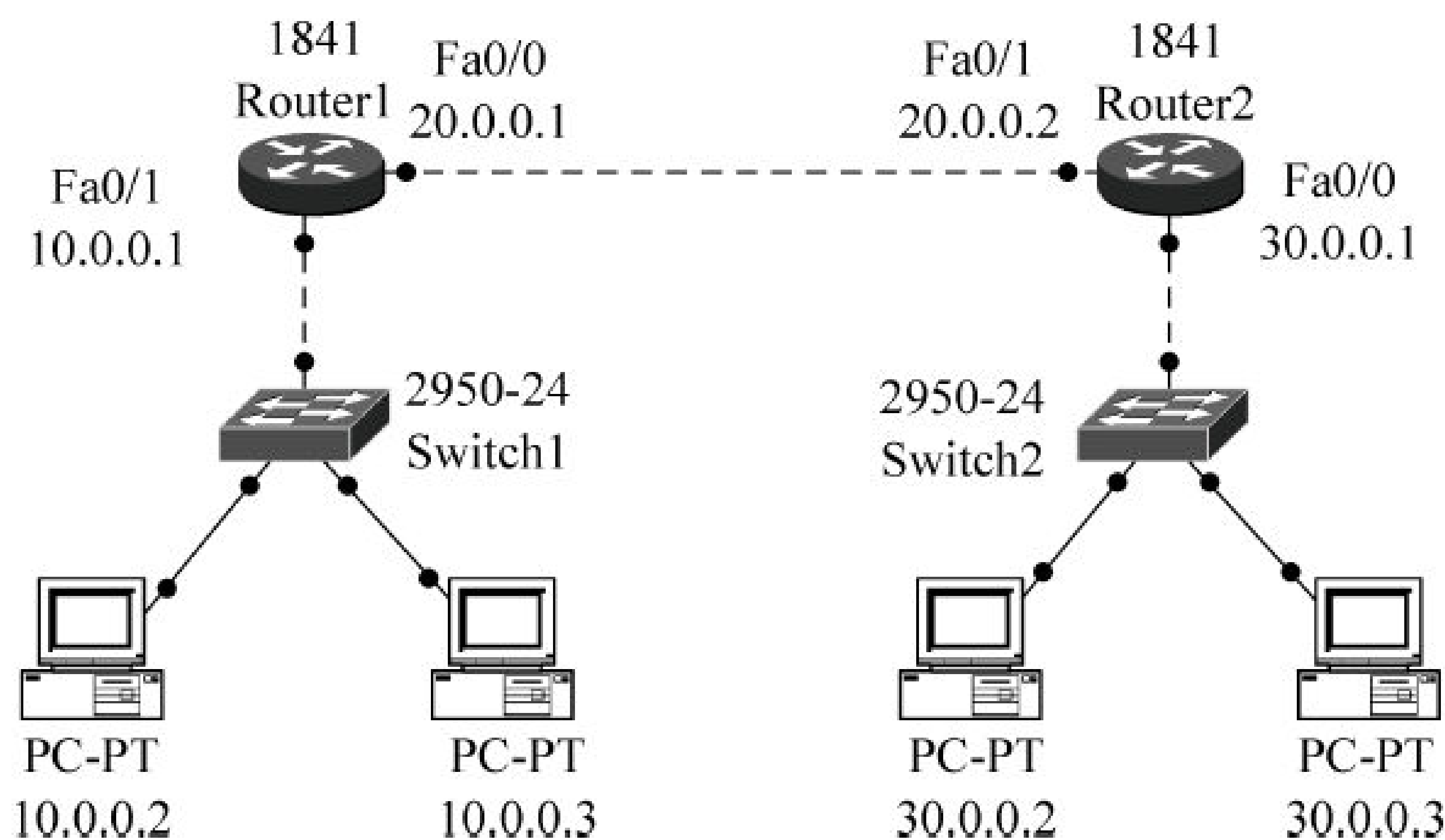


图 5-1 基本静态路由配置的网络环境

在本例中，首先用交叉线将两个路由器连接起来，然后用直通线将交换机 Switch1 分别与路由器 Router1 和各计算机连接起来；并用直通线将交换机 Switch2 分别与路由器 Router2 和各计算机连接起来；并按图 5-2 中所示的地址配置好每个设备的 IP 地址。值得提醒的是，在本例中，需要将 IP 地址为 10.0.0.2 和 10.0.0.3 的计算机的网关指定为 10.0.0.1；同时，还需要将 IP 地址为 30.0.0.2 和 30.0.0.3 的计算机的网关指定为 30.0.0.1。

此时，从 IP 地址为 10.0.0.2 的计算机 ping 30.0.0.0/8 网络中的设备，显然是不通的；反过来，从 IP 地址为 30.0.0.3 的计算机 ping 10.0.0.0/8 网络中的设备，也是不通的。原因是路由器 Router1 并不知道应通过哪条路径将数据包从 10.0.0.0/8 网络转发到网络 30.0.0.0/8；同样，路由器 Router2 也不知道应通过哪条路径将数据包从 30.0.0.0/8 网络转发到网络 10.0.0.0/8。路由器会将不知道转发路径的数据包丢弃。因此，计算机无法 ping 通跨越路由器的另一个网络。因此，我们必须为路由器 Router1 人工指定一条到达网络 30.0.0.0/8 的静态路由，具体方法是在路由器 Router1 的全局配置模式下输入如图 5-2 所示的命令。

```
Router1(config)#
Router1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2
Router1(config)#
```

图 5-2 为 Router1 指定下一跳 IP 地址静态路由

以上这条命令的含义是告诉路由器 Router1，对需要转发到网络 30.0.0.0/8 的所有数据包，使用下一跳 IP 地址为 20.0.0.2 这一条路径送出去。

请读者牢记，网络通信都是双向的。要实现双向通信，还需要为路由器 Router2 指定一条到达网络 10.0.0.0/8 的静态路由。请在路由器 Router2 下输入如图 5-3 所示的命令。

```
Router2(config)#
Router2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
Router2(config)#
```

图 5-3 为 Router2 指定下一跳 IP 地址静态路由

同理，以上这条命令的含义是告诉路由器 Router2 需要转发到网络 10.0.0.0/8 的所有数据包，都可以通过下一跳 IP 地址为 20.0.0.1 的路径送出去。

此时，可以通过命令 show ip route 来查看两个路由器的路由表，结果如图 5-4 和图 5-5 所示。在这两个图中，以字母 S 开头的一行信息就是配置成功的静态路由。

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mc
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    20.0.0.0/8 is directly connected, FastEthernet0/0
S    30.0.0.0/8 [1/0] via 20.0.0.2
Router1#
```

图 5-4 配置静态路由后路由器 Router1 的路由表

```
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mc
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

S    10.0.0.0/8 [1/0] via 20.0.0.1
C    20.0.0.0/8 is directly connected, FastEthernet0/0
C    30.0.0.0/8 is directly connected, FastEthernet0/1
Router2#
```

图 5-5 配置静态路由后的路由器 Router2 的路由表

此时，网络 10.0.0.0/8 与网络 30.0.0.0/8 已经连通了。可以在路由器 Router1 用 ping 命令来测试网络的连通性，测试结果如图 5-6 所示。

同样，可以在路由器 Router2 用 ping 命令来测试网络的连通性，测试结果如图 5-7 所示。

```
Router1#ping 30.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.0.0.1, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
```

图 5-6　用 ping 命令测试路由器 Router1 与网关的连通性

```
Router2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
```

图 5-7　路由器 Router2 连通性测试结果

配置静态路由时，除了以上介绍的用指定下一跳接口的 IP 地址的命令外，也可以用指定下一跳的送出接口名称的命令来实现。命令格式如下：

ip route 网络地址 子网掩码 送出接口名称

这里，我们仍以图 5-1 所示的网络环境为例，说明用指定送出接口名称的命令来配置静态路由的方法。对于路由器 Router1，具体配置命令如图 5-8 所示。

```
Router1(config)#
Router1(config)#ip route 30.0.0.0 255.0.0.0 Fa0/0
Router1(config)#
```

图 5-8　用送出接口名称为 Router1 指定静态路由

在图 5-8 所示的配置命令中，我们修改了最后一个参数，即用送出接口名称"Fa0/0"替代了图 5-2 中原来的"20.0.0.2"，实现了同样一条静态路由的配置。用命令 show ip route 查看路由器 Router1 的路由表，可以得到如图 5-9 所示的配置结果。

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mo
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    20.0.0.0/8 is directly connected, FastEthernet0/0
S    30.0.0.0/8 [1/0] via 20.0.0.2
                is directly connected, FastEthernet0/0
Router1#
```

图 5-9　用送出接口名称配置后的 Router1 路由表

此时，在路由器 Router1 同样用 ping 命令测试网络的连通性，也可以发现网络 10.0.0.0/8 与网络 30.0.0.0/8 已经连通了。测试结果如图 5-10 所示。

```
Router1#ping 30.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.0.0.1, timeout is 2 se
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =

Router1#
```

图 5-10 用送出接口名称配置后路由器 Router1 与网关的连通性测试

同理，对于路由器 Router2，用指定送出接口的名称“Fa0/1”来进行静态路由配置，具体命令如图 5-11 所示。

```
Router2(config)#
Router2(config)#ip route 10.0.0.0 255.0.0.0 Fa0/1
Router2(config)#
```

图 5-11 用送出接口名称为 Router2 指定静态路由

此时，用命令 show ip route 查看路由器 Router2 的路由表，也可以得到如图 5-12 所示的配置结果，表明配置成功。

```
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mo
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

S    10.0.0.0/8 [1/0] via 20.0.0.1
                is directly connected, FastEthernet0/0
C    20.0.0.0/8 is directly connected, FastEthernet0/0
C    30.0.0.0/8 is directly connected, FastEthernet0/1
Router2#
```

图 5-12 用送出接口名称配置后的路由器 Router2 的路由表

5.2 更复杂的 IPv4 静态路由配置

第 5.1 节已经介绍了只有两个路由器的网络环境下的最简单的静态路由的配置方法。但是，实际的互联网应用环境，不可能都像图 5-1 那么简单。下面进一步介绍对于更复杂的网络环境，如何进行 IPv4 静态路由配置。

在图 5-1 所示的网络环境基础上，本例增加了第 3 个路由器。各个网络设备的 IP 地址等网络参数如图 5-13 所示。其中，新增加的路由器 Router3 通过串行接口连接到路由器 Router2，并通过交换机分别连接到 IP 地址为 50.0.0.2 和 50.0.0.3 的计算机。

下一步需要进行静态路由配置。由于在网络中并没有使用任何动态路由，因此网络管理员必须在每台路由器上为其指明所有非直连网络的静态路由。

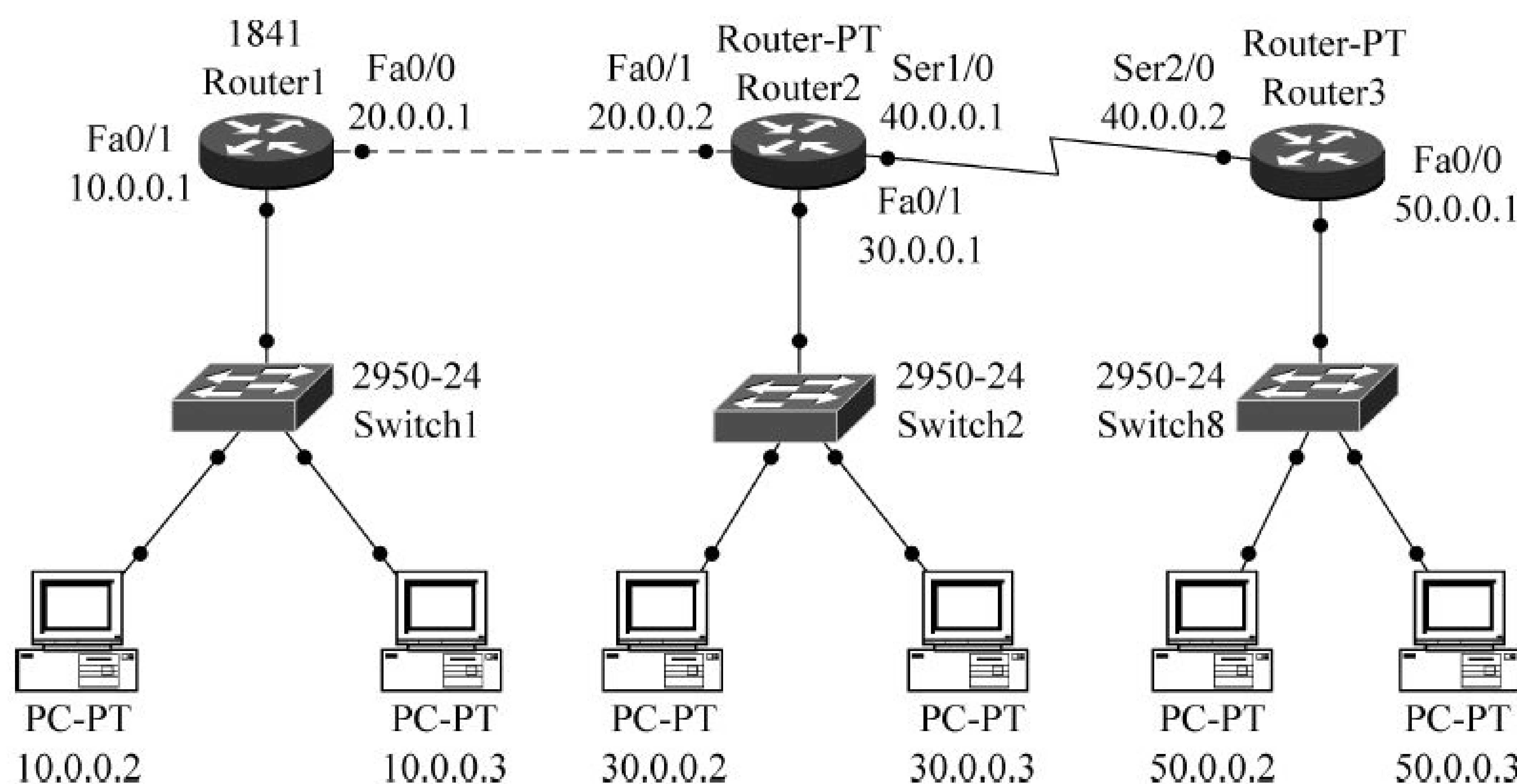


图 5-13 更复杂的静态路由配置网络环境

在图 5-13 所示的网络实验环境中，由于路由器 Router1 并没有与网络 30.0.0.0/8、40.0.0.0/8 和网络 50.0.0.0/8 直接连接，因此，网络管理员应当为路由器 Router1 逐一指定转发到网络 30.0.0.0/8、网络 40.0.0.0/8 和网络 50.0.0.0/8 的静态路由。具体的配置命令如图 5-14 所示。

```
Router1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2
Router1(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.2
Router1(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.2
Router1(config)#
```

图 5-14 配置路由器 Router1 静态路由的命令

同理，由于路由器 Router2 并没有与网络 10.0.0.0/8 和网络 50.0.0.0/8 直接连接，所以网络管理员也同样要为路由器 Router2 各自指定一条转发到网络 10.0.0.0/8 和网络 50.0.0.0/8 的静态路由。具体的配置命令如图 5-15 所示。

```
Router2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
Router2(config)#ip route 50.0.0.0 255.0.0.0 40.0.0.2
Router2(config)#
```

图 5-15 配置路由器 Router2 静态路由的命令

由于路由器 Router3 也没有与网络 10.0.0.0/8、网络 20.0.0.0/8 和 30.0.0.0/8 直接连接，因此，网络管理员也应当为路由器 Router3 逐一指定转发到网络 10.0.0.0/8、网络 20.0.0.0/8 和网络 30.0.0.0/8 的静态路由。具体的配置命令如图 5-16 所示。

```
Router3(config)#ip route 10.0.0.0 255.0.0.0 40.0.0.1
Router3(config)#ip route 20.0.0.0 255.0.0.0 40.0.0.1
Router3(config)#ip route 30.0.0.0 255.0.0.0 40.0.0.1
Router3(config)#
```

图 5-16 配置路由器 Router3 静态路由的命令

此时，这 3 个路由器都已经配置完成了，我们同样可以分别用命令 show ip route 来查看这 3 个路由器的路由表，命令的执行结果依次如图 5-17～图 5-19 所示。在这 3 个图中，以字母 S 开头的行信息就是配置成功的静态路由。

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mc
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    20.0.0.0/8 is directly connected, FastEthernet0/0
S    30.0.0.0/8 [1/0] via 20.0.0.2
                is directly connected, FastEthernet0/0
S    40.0.0.0/8 [1/0] via 20.0.0.2
S    50.0.0.0/8 [1/0] via 20.0.0.2
Router1#
```

图 5-17　3 个路由器都配置成功后的路由器 Router1 的路由表

```
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mc
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

S    10.0.0.0/8 [1/0] via 20.0.0.1
C    20.0.0.0/8 is directly connected, FastEthernet0/1
C    30.0.0.0/8 is directly connected, FastEthernet0/0
C    40.0.0.0/8 is directly connected, Serial1/0
S    50.0.0.0/8 [1/0] via 40.0.0.2
Router2#
```

图 5-18　3 个路由器都配置成功后的路由器 Router2 的路由表

```
Router3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mc
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

S    10.0.0.0/8 [1/0] via 40.0.0.1
S    20.0.0.0/8 [1/0] via 40.0.0.1
S    30.0.0.0/8 [1/0] via 40.0.0.1
C    40.0.0.0/8 is directly connected, Serial2/0
C    50.0.0.0/8 is directly connected, FastEthernet0/0
Router3#
```

图 5-19　3 个路由器都配置成功后的路由器 Router3 的路由表

图 5-17 表明，路由器 Router1 有 2 条直连路由（以字母 C 开头）和 3 条静态路由（以字母 S 开头）。

图 5-18 所示的路由表信息表明，路由器 Router2 有 3 条直连路由（以字母 C 开头）和 2 条静态路由（以字母 S 开头）。

同样，图 5-19 所示的路由表信息则表明，路由器 Router3 有 2 条直连路由（以字母 C 开头）和 3 条静态路由（以字母 S 开头）。

最后，我们可以逐一在每个路由器上用 ping 命令测试网络的连通性。这里，仅以路由器 Router1 为例来说明。在路由器 Router1 中用 ping 命令测试其与其他网络的计算机连通性，测试结果如图 5-20 所示，结果表明网络已经连接正常。

```
Router1#ping 30.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.0.0.2, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping 40.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.0.0.2, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping 50.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 50.0.0.2, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#
```

图 5-20 测试路由器 Router1 与各台计算机的连通性

5.3 汇总 IPv4 静态路由

汇总静态路由是一条可以用来表示多条静态路由的单独的路由。汇总静态路由通常是具有相同的送出接口或下一跳 IP 地址的连续网络的集合。

1. 用汇总静态路由简化路由表

较小的路由表可以使路由表查找过程更加有效率，因为需要搜索的路由条数更少。如果可以使用一条静态路由代替多条静态路由，就可以简化路由表。在许多情况下，一条汇总静态路由可以替代几十条、几百条，甚至几千条静态路由。

我们可以使用一个网络地址代表多个子网。例如，172.0.0.0/16、172.1.0.0/16、172.2.0.0/16、172.3.0.0/16、172.4.0.0/16、172.5.0.0/16、172.6.0.0/16……直到网络地址 172.255.0.0/16，所有这些地址都可以用一个汇总的网络地址 172.0.0.0/8 来表示。

2. 汇总静态路由的条件

多条静态路由可以汇总成一条静态路由，前提是符合以下条件：

（1）多个目的网络地址可以汇总成一个网络地址。

（2）多条静态路由都使用相同的下一跳 IP 地址和相同的送出接口。

以图 5-21 所示的网络环境为例，路由器 Router3 有 3 条静态路由。所有 3 条静态路由都通过相同的下一跳地址 192.168.1.1 和相同的送出接口 Ser2/0 转发数据包。

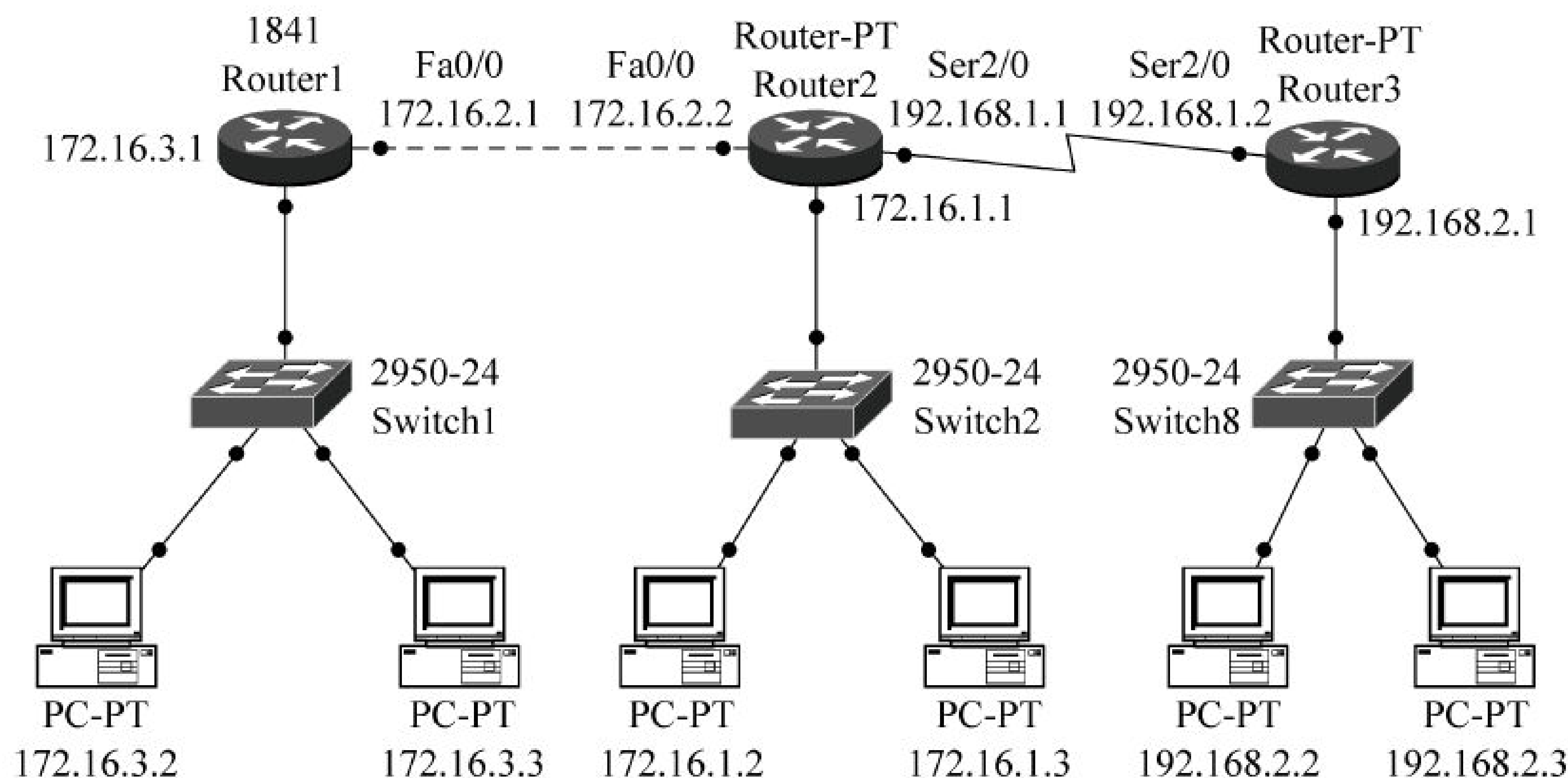


图 5-21　可以汇总静态路由的网络环境

路由器 Router3 的这 3 条静态路由原来是分别配置的，如图 5-22 所示。

```
Router3(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.1
Router3(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.1
Router3(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.1
```

图 5-22　路由器 Router3 的 3 条静态路由

现在，我们将这 3 条静态路由汇总成一条静态路由，即将 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24 这 3 个子网地址汇总成网络地址 172.16.0.0/22。因为这 3 条路由都使用相同的下一跳地址和相同的送出接口，所以我们可以将其简化为一条汇总的静态路由，网络地址为 172.16.0.0，子网掩码为 255.255.252.0。

在配置汇总静态路由之前，我们必须首先删除原来的 3 条静态路由，如图 5-23 所示。

```
Router3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.1
Router3(config)#no ip route 172.16.2.0 255.255.255.0 192.168.1.1
Router3(config)#no ip route 172.16.3.0 255.255.255.0 192.168.1.1
```

图 5-23　删除当前路由器 Router3 的 3 条静态路由

这时可以用 show ip route 命令查看路由器 Router3 当前的路由表，如图 5-24 所示。

下一步，我们就可以配置汇总的静态路由，即仅用一条统一的汇总路由配置命令，就可以替代图 5-22 所示的 3 条静态路由，如图 5-25 所示。

此时，就可以用 show ip route 命令查看路由器 Router3 的汇总静态路由表，如图 5-26 所示。

在图 5-26 中，可以看到“S　172.16.0.0 [1/0] via 192.168.1.1”这一条汇总，表明已经配置成功。

通过这条汇总路由，数据包的目的 IP 地址仅需要与 172.16.0.0 网络地址最左侧的 22

```
Router3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, I
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter a
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external typ
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - I
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Serial2/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
Router3#
```

图 5-24　路由器 Router3 当前的路由表

```
Router3(config)#ip route 172.16.0.0 255.255.252.0 192.168.1.1
Router3(config)#
```

图 5-25　汇总路由配置命令

```
Router3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, I
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter a
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external typ
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - I
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/22 is subnetted, 1 subnets
S       172.16.0.0 [1/0] via 192.168.1.1
C    192.168.1.0/24 is directly connected, Serial2/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
Router3#
```

图 5-26　路由器 Router3 的汇总静态路由表

位匹配。目的 IP 地址属于 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24 网络的所有数据包都与这条汇总路由匹配。

同理，在图 5-21 所示的网络环境中，路由器 Router1 的两条静态路由 192.168.1.0/24、192.168.2.0/24 也可以汇总成一条路由 192.168.0.0/22。具体的配置方法相似，这里，我们就不作详细介绍了，请读者自行练习。

最后，可以使用 ping 命令测试网络的连通性，即分别使用 ping 命令测试与网络 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24 的连接情况，测试结果如图 5-27 所示。

从图 5-27 中可以发现，从每个路由器发出的数据包都能够到达其目的地，并且返回路径也工作正常。

```
Router3#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/

Router3#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/

Router3#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/37/

Router3#
```

图 5-27 测试网络的连通性

5.4 IPv4 默认静态路由

当网络互联的规模很大时，采用静态路由或者动态路由，都难以实现对所有远程网络路由的穷尽。限制主要来自路由存储空间、路由更新维护成本、路由查收速度，以及对远程网络的拓扑结构不了解等，此时就需要配置默认静态路由。

这里，我们以图 5-28 所示的末节网络为例，来说明默认静态路由。

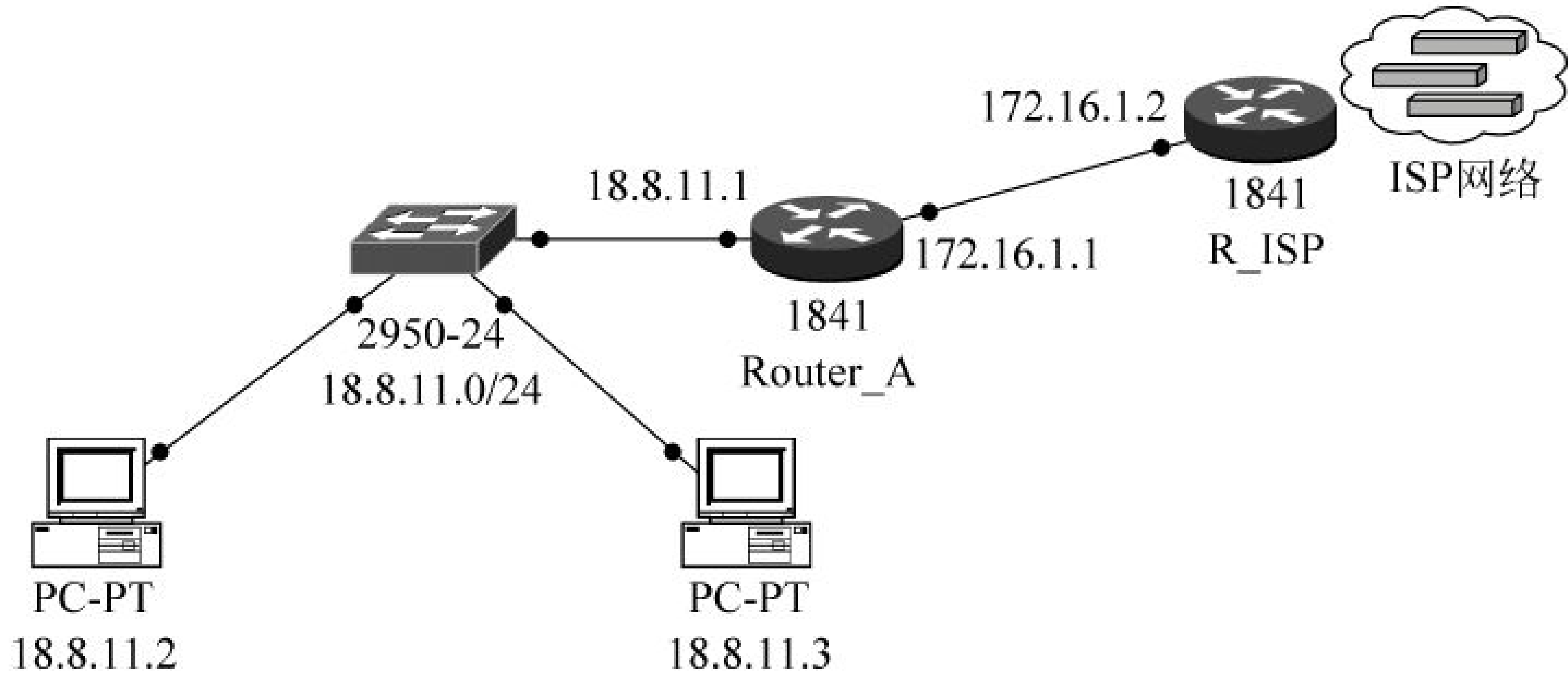


图 5-28 末节网络

只有一条路径可以到达的网络称为末节网络，也称为孤岛网络。在图 5-28 所示的末节网络环境中，网络服务商的路由器 R_ISP 在为某企业网络 18.8.11.0/24 配置路由时，就需要使用默认静态路由。

作为企业网络的边界路由器 Router_A，企业中所有计算机发送到 Internet 的数据包都需要通过路由器 Router_A 转发，如果路由器 Router_A 为 Internet 上百万个以上的目标网络都保存其路由信息，路由器 Router_A 就会出现路由表“爆炸”，不仅需要大量的内存空间和路由更新维护的成本，路由器的性能也会急剧下降。

为了解决这个问题，引入了默认静态路由（Default Static Route）的概念。默认静态路由也称为默认路由。作为一种特殊的静态路由，默认静态路由配置命令中的网络地址和子网掩码都是 0.0.0.0。对于一个路由器来说，进行路由匹配查找时，首先要根据转发数据包的目标地址，在路由表中逐条进行查找，如果找不到任何明确的匹配项，默认静态路由指定的路由就是最后的选择，即当路由器从当前路由表中找不到数据包目标地址匹配的路由条目时，就把数据包送到默认静态路由指定的路由器下一跳 IP 地址或者送出接口。

在路由器 Router_A 的全局配置模式下，输入如图 5-29 所示的命令，即可配置默认静态路由。

```
Router_A(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
Router_A(config)#
```

图 5-29　默认静态路由配置命令

接着，可以使用 show ip route 命令查看路由表，结果如图 5-30 所示。

```
Router_A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mc
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

C    18.0.0.0/8 is directly connected, FastEthernet0/1
C    172.16.0.0/16 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.16.1.2
Router_A#
```

图 5-30　默认静态路由表

请注意图 5-30 中字母 S 旁边的星号（*），星号表明这条静态路由是一条默认静态路由，其下一跳 IP 地址是 172.16.1.2。

默认静态路由配置的关键在于/0 子网掩码。路由表中的子网掩码决定着数据包的目的 IP 地址与路由表中的路由之间必须有多少位匹配。而/0 子网掩码表明只需要零位匹配，即不需要匹配。

默认静态路由在路由器配置时十分常用。这样，路由器就不需要存储通往 Internet 中所有网络的路由，而只用一条默认路由就可以代表不在路由表中的任何网络。

5.5　IPv4 浮动静态路由

当某一条静态路由出现故障时，原来所有需要通过这条路由的数据包都无法正常传输。此时，就只能由网络管理员重新配置静态路由来应对网络故障。这样，如果网络的规模很大、很复杂，则网络管理员的工作量将会很大。

那么，针对这种静态路由可能出现故障的情况，网络管理员有没有相应的解决方法呢？答案是配置浮动静态路由。配置浮动静态路由，是指同时在两个路由器之间配置两条甚至更多的备份网络链路。

这里，我们以图 5-31 所示的网络环境来说明如何配置浮动静态路由。

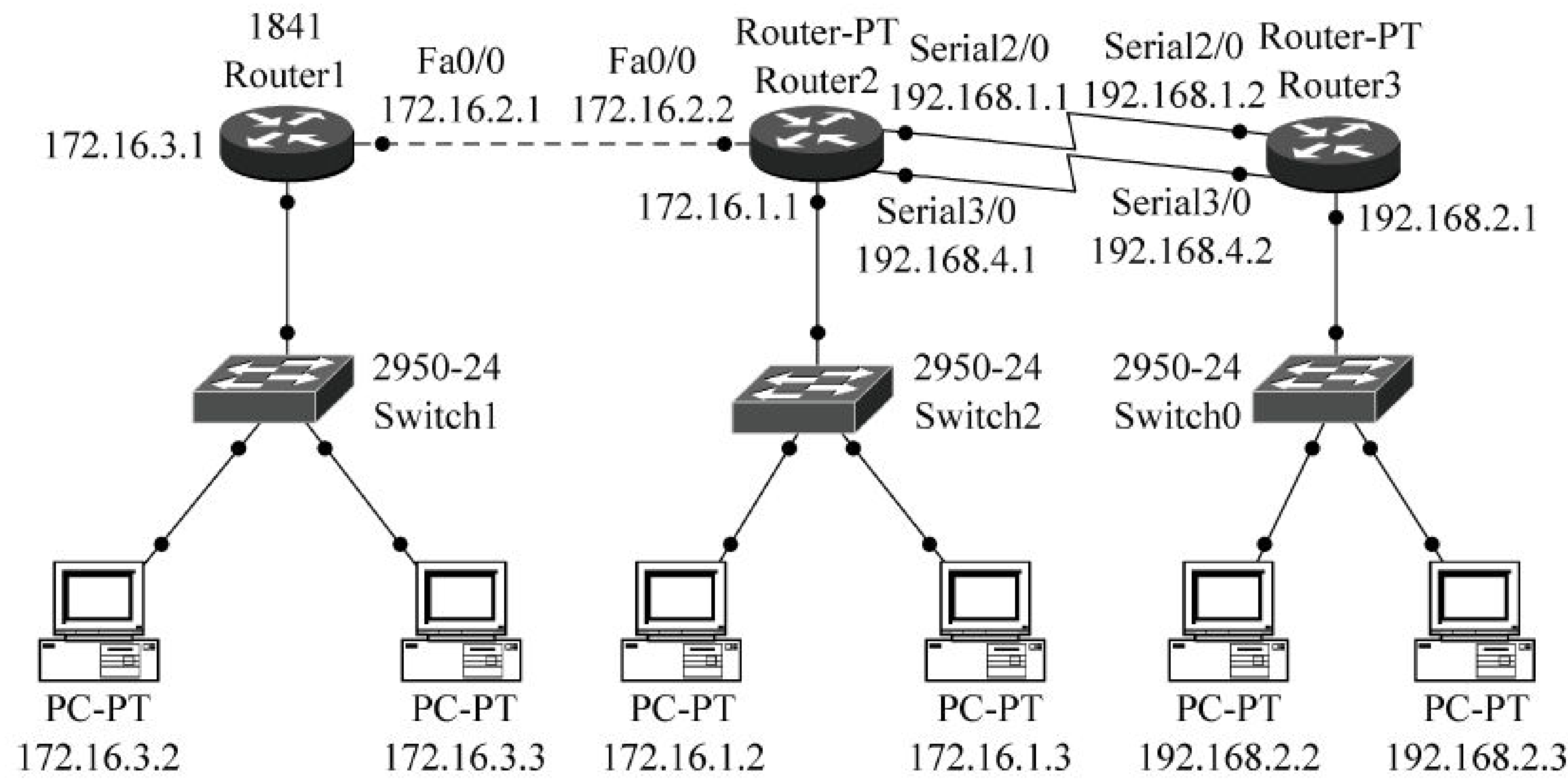


图 5-31 配置浮动静态路由的网络环境

在图 5-31 中，路由器 Router2 与路由器 Router3 之间连接了 2 条串行通信链路：一条是 192.168.1.0/24；另一条是 192.168.4.0/24。

配置浮动静态路由的命令格式是如下两条命令之一：

```
ip route 网络地址 子网掩码 下一跳地址 [管理距离]
ip route 网络地址 子网掩码 送出接口名称 [管理距离]
```

默认情况下，静态路由的管理距离为 1，如果想通过备份链路实现冗余的静态路由，只要以这条备份路径的下一跳地址，加上一个管理距离数值(1～255)来配置浮动路由即可。

在路由器 Roter3 的全局配置模式下，可以使用如图 5-32 所示的命令为其配置浮动静态路由。在本例中，浮动路由是 192.168.4.1，管理距离为 10。

```
Router3(config)#ip route 172.16.0.0 255.255.0.0 192.168.1.1
Router3(config)#ip route 172.16.0.0 255.255.0.0 192.168.4.1 10
Router3(config)#
```

图 5-32 配置浮动静态路由

配置后，用 show ip route 命令查看浮动静态路由的配置结果，则路由器 Router3 的路由表如图 5-33 所示。

```
Router3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inte
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       * - candidate default, U - per-user static route, o - ODI
       P - periodic downloaded static route

Gateway of last resort is not set

S    172.16.0.0/16 [1/0] via 192.168.1.1
C    192.168.1.0/24 is directly connected, Serial2/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial3/0
Router3#
```

图 5-33 查看浮动静态路由的配置结果

但是，在图 5-33 中，我们并没有找到刚才配置的浮动路由。这是为什么呢？原因很简单，这是因为我们配置的两条路径的管理距离值不一样，一条路径的管理距离值取默认值“1”，另一条路径的管理距离值设置为“10”，而管理距离值较小的路径被路由器作为优先选择的路由。所以，当前只有 192.168.1.1 这一条路由。

为了让浮动静态路由生效，用 shutdown 命令关闭路由器 Router3 的串行接口 Serial2/0，具体操作命令如图 5-34 所示。

```
Router3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router3(config)#interface Serial2/0
Router3(config-if)#shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to administrati
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed

Router3(config-if)#exit
Router3(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router3#
```

图 5-34　关闭路由器 Router3 的串行接口 Serial2/0

然后，再次通过命令 show ip route 查看路由表，结果如图 5-35 所示。

```
Router3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter ar
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EG
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-I
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    172.16.0.0/16 [10/0] via 192.168.4.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial3/0
Router3#
```

图 5-35　配置浮动静态路由的结果

从图 5-35 中可以看到，这条管理距离设为“10”的浮动静态路由，终于浮现在我们的眼前。

5.6　负载均衡

在以上浮动静态路由的配置实例中，当路由器转发数据包时，是无法同时使用这两条链路的。仅当第一条链路不起作用时，第二条链路才会工作。换句话说，在以上的配置实例中，对于要前往目的地的数据包来说，即使两条链路都是完好的，也有一条链路没法正常使用。这显然是对链路资源的一种浪费。那么，能否物尽其用，让与路由器连接的两条链路同时工作呢？

答案是肯定的，其解决方法是负载均衡。其实，要实现负载均衡的方法很简单，就是将

转发到同一目标地址的两条链路的管理距离设置为相同的数值。这样,路由器就会使这两条链路同时生效,均衡地分担网络的数据流量。

例如,对于图 5-31 所示的网络环境,负载均衡的具体配置方法如图 5-36 所示。

```
Router3(config)#ip route 172.16.0.0 255.255.0.0 192.168.1.1 2
Router3(config)#ip route 172.16.0.0 255.255.0.0 192.168.4.1 2
Router3(config)#
```

图 5-36 配置负载均衡的静态路由

在图 5-36 所示的实例中,我们将需要实现转发到目标地址 172.16.0.0 的两条路径的管理距离的数值都设置为"2",从而实现了负载均衡。

配置完成后,可以使用命令 show ip route 来查看刚才配置好的路由表,结果如图 5-37 所示。

```
Router3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter ar
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EG
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-I
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    172.16.0.0/16 [2/0] via 192.168.1.1
                   [2/0] via 192.168.4.1
C    192.168.1.0/24 is directly connected, Serial2/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial3/0
Router3#
```

图 5-37 配置负载均衡的静态路由的结果

从图 5-37 中可以看到,路由器 Router3 前往同一个目标网络 172.16.0.0/16 的路由,同时有两个下一跳地址(即 192.168.1.1 和 192.168.4.1)可供使用。这表明,当路由器转发前往同一目标网络的数据包时,就会同时使用这两个下一跳地址进行转发,即可以实现负载均衡。

5.7 配置 IPv6 静态路由和默认路由

不论是 IPv4,还是 IPv6 的网络环境,都完整地支持静态路由。如上所述,静态路由是指由网络管理员手工配置的路由信息。但是,当网络的拓扑结构或链路的状态发生变化时,需要网络管理员人工修改路由表中的相关静态路由信息。静态路由信息在默认情况下是私有的,不会传递给其他路由器。

配置 IPv6 网络环境的静态路由的方法与 IPv4 网络环境的命令很相似,只要将原来命令中的字符串 IP 修改为相应的 IPv6 即可。

配置 IPv6 网络,首先要在路由器的全局配置模式下输入以下命令,启动 IPv6 的单播功能。

```
ipv6 unicast - routing
```

接着，指定一个需要配置的路由器接口，并给这个接口配置 IPv6 地址和子网掩码。命令格式如下。

```
interface 接口名称
ipv6 address 网络地址/子网掩码
```

最后，用以下命令激活接口。

```
no shutdown
```

路由器的 IPv6 地址配置完成后，就可以使用以下命令配置静态路由了。

```
ipv6 route 网络地址 子网掩码 下一跳地址/送出接口名称
```

下面以图 5-38 所示的 IPv6 网络环境为例，介绍 IPv6 的静态路由的配置方法。

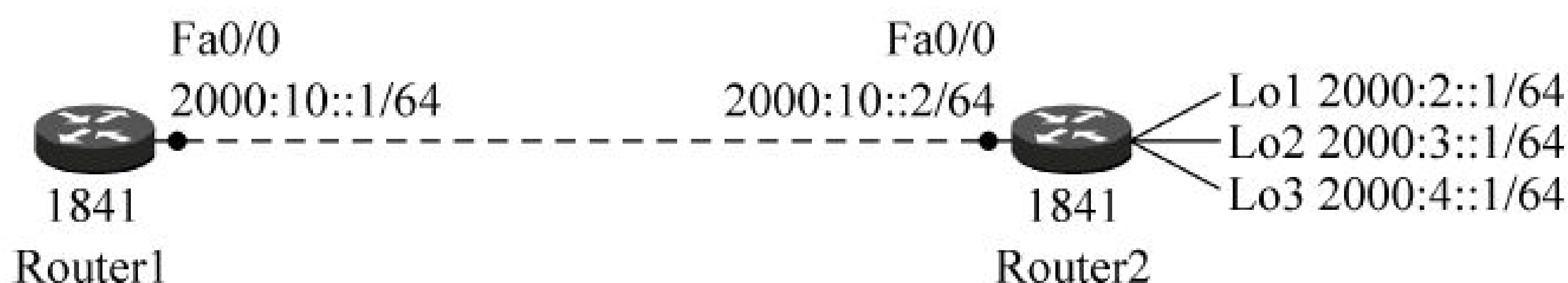


图 5-38　IPv6 网络环境

首先，在路由器 Router1 的全局配置模式下，为快速以太网接口 FastEthernet0/0 配置 IPv6 地址，并激活接口，具体操作如图 5-39 所示。

```
Router1(config)#ipv6 unicast-routing
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ipv6 address 2000:10::1/64
Router1(config-if)#no shutdown
Router1(config-if)#
```

图 5-39　路由器 Router1 的 IPv6 地址配置

接着，在路由器 Router2 的全局配置模式下，为快速以太网接口 FastEthernet0/0 配置 IPv6 地址，并激活接口，具体操作如图 5-40 所示。

```
Router2(config)#ipv6 unicast-routing
Router2(config)#interface FastEthernet0/0
Router2(config-if)#ipv6 address 2000:10::2/64
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#
```

图 5-40　路由器 Router2 的 IPv6 地址配置

然后，为路由器 Router2 配置 3 个环回接口地址，分别模拟 3 个不同的 IPv6 前缀，作为 IPv6 的目标网络，具体操作如图 5-41 所示。

此时，在路由器 Router1 上用 ping 命令测试与两个直连接口（即地址 2000:10::1 和地址 2000:10::2）的连通性，结果可以 ping 通。而 ping 路由器 Router2 的环回地址（即地址 2000:2::1），结果 ping 不通，因为我们仍未在路由器 Router1 上配置到达 3 个环回地址的静态路由。ping 命令的连通性测试结果如图 5-42 所示。

下一步，在路由器 Router1 上配置到达 3 个环回地址的静态路由，如图 5-43 所示。

```
Router2(config)#interface loopback 1

%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
Router2(config-if)#ipv6 address 2000:2::1/64
Router2(config-if)#exit
Router2(config)#interface loopback 2

%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2,
Router2(config-if)#ipv6 address 2000:3::1/64
Router2(config-if)#exit
Router2(config)#interface loopback 3

%LINK-5-CHANGED: Interface Loopback3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback3,
Router2(config-if)#ipv6 address 2000:4::1/64
Router2(config-if)#exit
```

图 5-41 路由器 Router2 的 IPv6 环回地址配置

```
Router1#ping 2000:10::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:10::1, timeout is 2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping 2000:10::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:10::2, timeout is 2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping 2000:2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:2::1, timeout is 2 s
.....
Success rate is 0 percent (0/5)

Router1#
```

图 5-42 ping 命令的连通性测试结果

```
Router1(config)#ipv6 route 2000:2::/64 2000:10::2
Router1(config)#ipv6 route 2000:3::/64 2000:10::2
Router1(config)#ipv6 route 2000:4::/64 2000:10::2
Router1(config)#
```

图 5-43 配置到达 3 个环回地址的静态路由

当完成上述配置后，可以在路由器 Router1 上用 show ipv6 route 查看 IPv6 的路由表，结果如图 5-44 所示。

此时，在图 5-44 中可以清晰地看到 3 条被添加的静态路由。然后，在路由器 Router1 上再次测试与目标 IPv6 地址的连通性，应该成功连通，结果如图 5-45 所示。

下面为路由器 Router1 配置 IPv6 的默认静态路由。默认静态路由的 IPv6 地址为“::/0”，具体操作如图 5-46 所示。

```
Router1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - E
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, C
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   2000:2::/64 [1/0]
     via ::, FastEthernet0/0
     via 2000:10::2
S   2000:3::/64 [1/0]
     via ::, FastEthernet0/0
     via 2000:10::2
S   2000:4::/64 [1/0]
     via ::, FastEthernet0/0
     via 2000:10::2
C   2000:10::/64 [0/0]
     via ::, FastEthernet0/0
```

图 5-44　用 show ipv6 route 查看 IPv6 的路由表

```
Router1#ping 2000:2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:2::1, timeout is 2 s
!!!!!
Success rate is 60 percent (3/5), round-trip min/avg/max =

Router1#ping 2000:3::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:3::1, timeout is 2 s
!!!!!
Success rate is 60 percent (3/5), round-trip min/avg/max =
```

图 5-45　用 ping 命令测试连通性

```
Router1(config)#ipv6 route ::/0 2000:10::2
Router1(config)#
```

图 5-46　配置 IPv6 的默认静态路由

最后，可以用 show ipv6 route 查看路由表，结果如图 5-47 所示。从图 5-47 中可以看出，路由器 Router1 的默认路由已经配置成功。

```
Router1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - E
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, C
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
     via 2000:10::2
S   2000:2::/64 [1/0]
     via ::, FastEthernet0/0
S   2000:3::/64 [1/0]
     via ::, FastEthernet0/0
S   2000:4::/64 [1/0]
     via ::, FastEthernet0/0
C   2000:10::/64 [0/0]
```

图 5-47　路由器 Router1 的 IPv6 路由表

5.8 本章总结

静态路由是在路由器中设置的固定的路由表，即由网络管理员指定的固定的传输路径。除非网络管理员干预，否则静态路由不会自动更改。所以，当网络的拓扑结构或链路的状态发生变化时，需要网络管理员手工修改路由表中的相关静态路由信息。

静态路由配置可以在全局配置模式下输入以下两条配置命令之一：

```
ip route 网络地址 子网掩码 下一跳地址
ip route 网络地址 子网掩码 送出接口名称
```

请读者牢记，网络通信都是双向的。要实现双向通信，需要对通信双方的路由器分别指定静态路由。

静态路由配置完成后，可以分别在每个路由器上用命令 show ip route 来查看路由表，并用 ping 命令测试网络的连通性。

汇总静态路由是一条可以用来表示多条静态路由的单独的路由。汇总静态路由通常是具有相同的送出接口或下一跳 IP 地址的连续网络的集合。

多条静态路由可以汇总成一条静态路由，前提是须符合以下条件：

(1) 多个目的网络地址可以汇总成一个网络地址。

(2) 多条静态路由都使用相同的下一跳 IP 地址或相同的送出接口。

作为一种特殊的静态路由，默认静态路由配置命令中的网络地址和子网掩码都是 0.0.0.0。对于一个路由器来说，进行路由匹配查找时，首先要根据转发数据包的目标地址，在路由表中逐条进行查找，如果找不到任何明确的匹配项，默认静态路由指定的路由就是最后的选择，即当路由器从当前路由表中找不到数据包目标地址匹配的路由条目时，就把数据包送到默认静态路由指定的路由器下一跳 IP 地址或者送出接口。

配置浮动静态路由，是指同时在两个路由器之间配置两条甚至更多的备份网络链路。

配置浮动静态路由的命令格式是如下两条命令之一：

```
ip route 网络地址 子网掩码 下一跳地址 [管理距离]
ip route 网络地址 子网掩码 送出接口名称 [管理距离]
```

负载均衡是指让连接在两个路由器之间配置两条甚至更多的备份网络链路同时工作。实现负载均衡的方法很简单，就是将两条转发到同一目标地址的多条链路的管理距离设置为相同的数值。

配置 IPv6 网络环境的静态路由的方法与 IPv4 网络环境的命令很相似，只要将原来命令中的字符串 IP 修改为相应的 IPv6 即可。

配置 IPv6 网络，首先需要在路由器的全局配置模式下输入以下命令，启动 IPv6 的单播功能。

```
ipv6 unicast - routing
```

接着，指定一个需要配置的路由器接口，并给这个接口配置 IPv6 地址和子网掩码。命令格式如下。

```
interface 接口名称
ipv6 address 网络地址/子网掩码
```

最后，用以下命令激活接口。

```
no shutdown
```

路由器的 IPv6 地址配置完成后，就可以使用以下命令配置静态路由了。

```
ipv6 route 网络地址 子网掩码 下一跳地址/送出接口名称
```

复习思考题

1. 什么是静态路由？静态路由有什么特点？
2. 配置 IPv4 静态路由的两种命令格式是什么？
3. 如何查看 IPv4 路由表？
4. 什么是汇总静态路由？如何实现汇总静态路由？
5. 什么是默认静态路由？如何配置 IPv4 默认静态路由？
6. 什么是浮动静态路由？如何配置 IPv4 浮动静态路由？
7. 什么是负载均衡？如何实现负载均衡？
8. 如何配置 IPv6 静态路由和默认路由？
9. 如何查看 IPv6 路由表？
10. 如何测试 IPv4 网络的连通性？
11. 实训操作题 1：请按图 5-48 配置 3 个路由器的 IPv4 静态路由（负载均衡）。

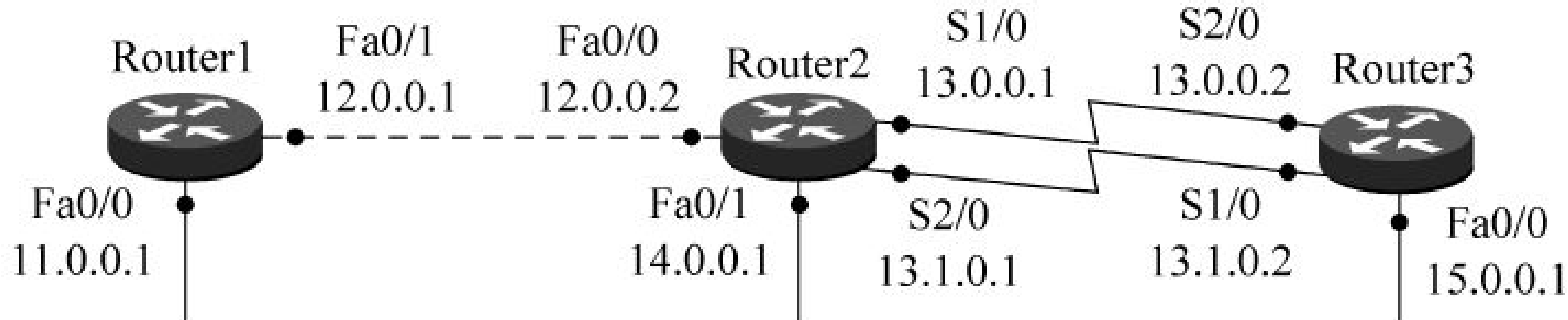


图 5-48　IPv4 静态路由（负载均衡）的网络环境

12. 实训操作题 2：请按图 5-49 配置 3 个路由器的 IPv6 静态路由。

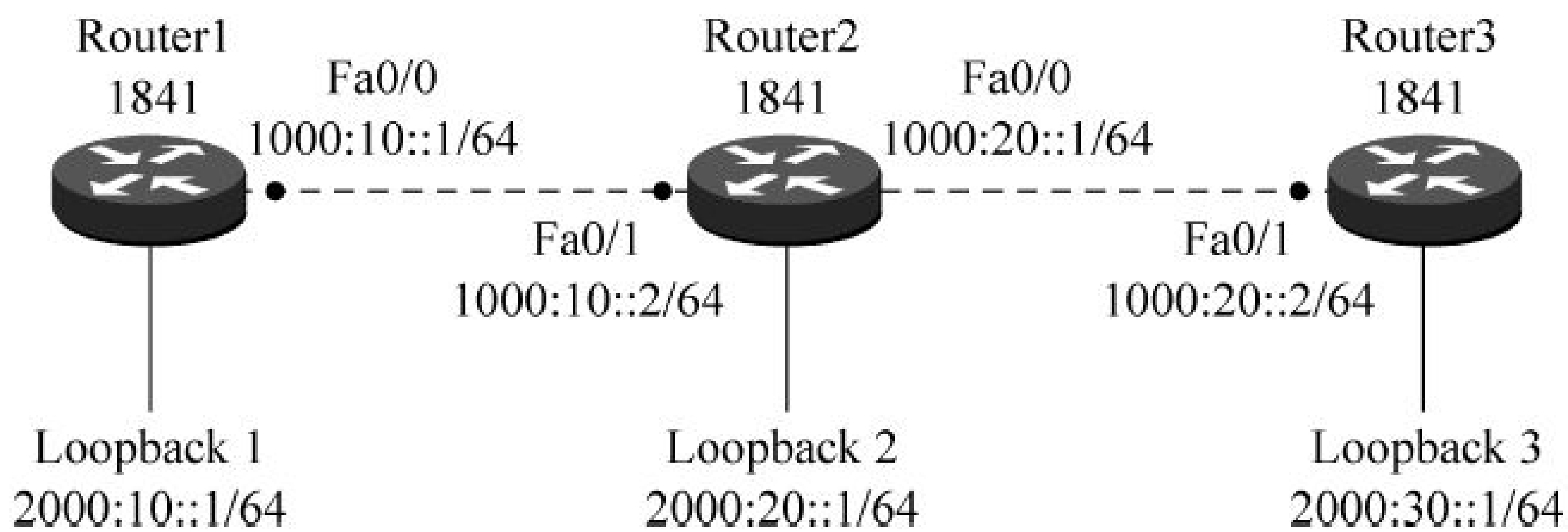


图 5-49　IPv6 静态路由的网络环境

第 6 章

CHAPTER 6

RIP

路由信息协议(Routing Information Protocol,RIP)是应用较早、使用较普遍的内部网关协议(Interior Gateway Protocol,IGP),适用于小型同类网络的一个自治系统(AS)内的路由信息的传递。RIP 是基于距离矢量算法(Distance Vector Algorithms,DVA)的。它使用“跳数”,即 metric 作为度量值来衡量到达目标地址的路由距离。目前,RIP 的最新版本是 RIPng,支持 IPv6 协议。

RIP 是最早的距离矢量路由协议。虽然 RIP 缺少许多更为高级的路由协议所具备的复杂功能,但正是因为它的简单性和实用性,使得它具有顽强的生命力。因此,我们不能因为它的工作原理简单就声称它是“即将被淘汰”的协议。事实上,目前已经开发了支持 IPv6 协议的 RIPng(ng 的含义是 next generation)协议,即下一代的 RIP。

6.1 RIP 的发展简史

RIP 的发展简史如图 6-1 所示。

RIP 是从美国 Xerox 公司开发的早期协议,即网关信息协议(GateWay INFOrmation Protocol,GWINFO)演变和发展而来的。从 20 世纪 70 年代起,随着 Xerox 网络服务(Xerox Networking Services,XNS)的发展,网关信息协议(GWINFO)逐渐发展成 RIP。此后,由于 UNIX 操作系统的优秀版本伯克利软件发行版(Berkeley Software Distribution,BSD)中的守护程序 routed(注:读作 route-dee,而不是 rout-ed)采用了 RIP,因此使得 RIP 随着 BSD 在全球的广泛应用而流行起来。此后,其他计算机厂商也相继开发出了大同小异的 RIP 版本。由于意识到需要对该协议进行标准化,所以 Charles Hedrick 在 1988 年编写了 RFC 1058,他在该文档中阐述了现有的 RIP 并进行了一些改进。从那时开始,RIP 逐步完善,1994 年开发了 RIPv2 协议,到了 1997 年,支持 IPv6 的 RIPng 协议正式问世。

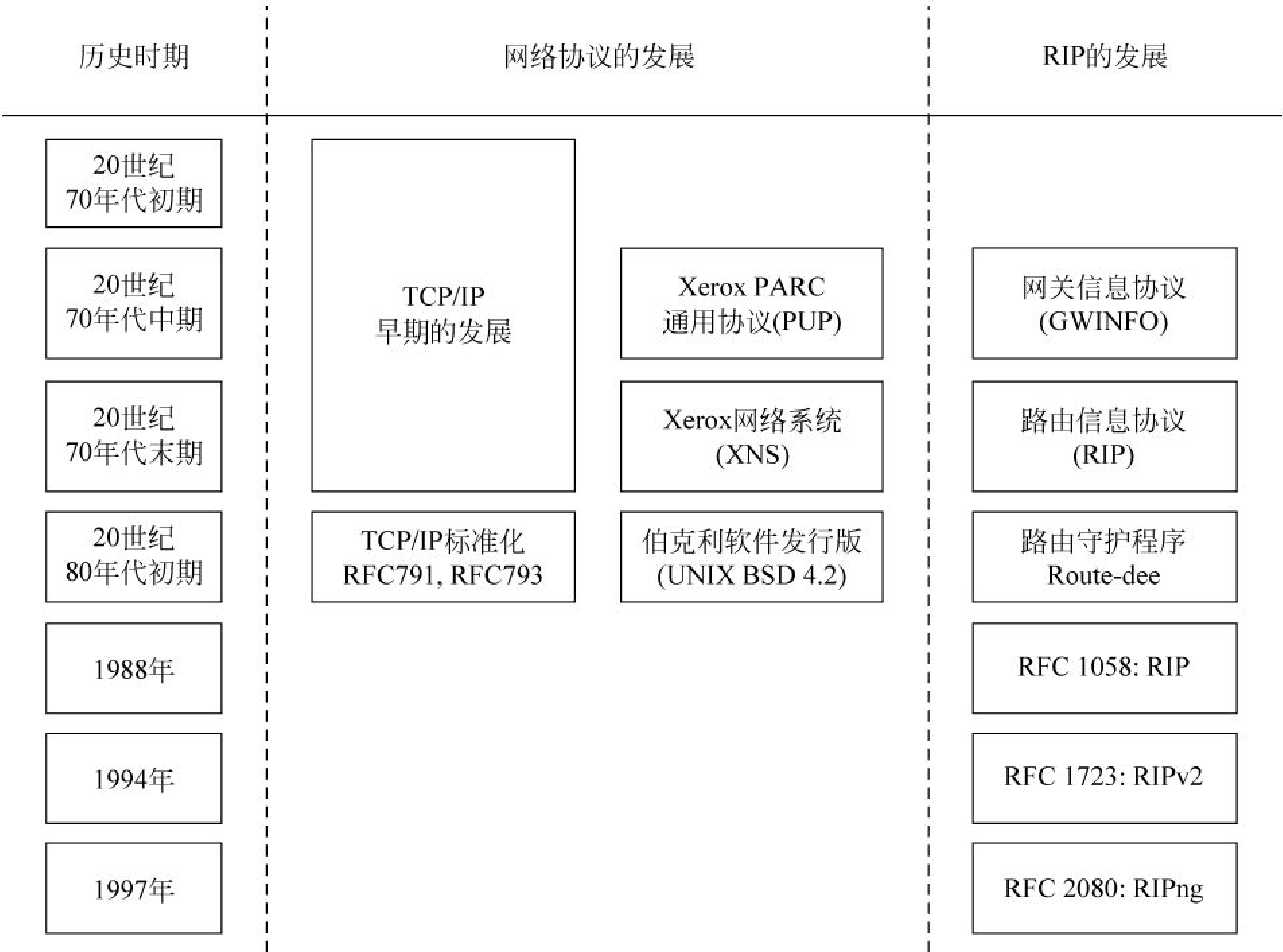


图 6-1 RIP 的发展简史

6.2 距离矢量路由协议

距离矢量路由协议采用贝尔曼-福特(Bellman-Ford)算法。常见的距离矢量路由协议分别是 RIP、IGRP、EIGRP 和 BGP 等。

1. RIP

路由信息协议(Routing Information Protocol,RIP)最早于 1988 年在 RFC 1058 中定义。RIP 主要有以下技术特点:

(1) 使用跳数作为选择路径的度量。

(2) 如果某个网络的跳数超过 15,RIP 便认为目的不可达,并删除该路由。

(3) 默认情况下,每隔 30s 通过广播或组播发送一次路由更新信息。

2. IGRP

内部网关路由协议(Interior Gateway Routing Protocol,IGRP)是由思科公司开发的专用协议。IGRP 的主要技术特点如下:

(1) 使用基于带宽、延迟、负载和可靠性的复合度量。

(2) 默认情况下,每隔 90s 通过广播发送一次路由更新信息。

(3) IGRP 是 EIGRP 的前身,思科路由器目前已经停止使用 IGRP 了。

3. EIGRP

增强型内部网关路由协议(Enhanced Interior Gateway Routing Protocol,EIGRP)也是

思科公司开发的专用的距离矢量协议。其主要技术特点如下：

（1）能够执行不等价负载均衡。

（2）使用扩散更新算法(Diffusing Update Algorithm，DUAL)计算最短路径。

（3）EIGRP 不需要像 RIP 和 IGRP 那样进行定时更新。只有当拓扑结构发生变化时，才会发送路由更新信息。

4．BGP

边界网关协议(Border Gateway Protocol，BGP)是运行于 TCP 上的一种自治系统的路由协议。BGP 是唯一一个用来处理像因特网大小的网络的协议，也是唯一能够妥善处理好不相关路由域间的多路连接的协议。BGP 构建在外部网关协议(Exterior Gateway Protocol，EGP)的经验之上。BGP 系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括列出的自治系统(AS)的信息。这些信息有效地构造了 AS 互联的拓扑图，并由此清除了路由环路，同时在 AS 级别上可实施策略决策。

6.3 距离矢量路由算法

距离矢量路由算法的基本思想如下：每个路由器维护一个距离矢量(通常是用延时的长短计算)表，然后通过相邻路由器之间的距离矢量通告进行距离矢量表的更新。每个距离矢量表项包括两部分：到达目的结点的最佳输出线路；到达目的结点所需的时间或距离，通信子网中的其他每个路由器在表中占据一个表项，并作为该表项的索引。每隔一段时间，路由器会向所有邻居结点发送它到每个目的结点的距离表，同时它也接收每个邻居结点发来的距离表。以此类推，经过一段时间后，便可将网络中各路由器获得的距离矢量信息在各路由器上统一起来，这样各路由器只需要查看这个距离矢量表，就可以为不同来源分组找到一条最佳的路由。

我们首先以图 6-2 所示的网络环境为例，来说明距离矢量路由算法。假设某个时候路由器 Router2 收到其邻居路由器 Router1 的距离矢量，其中 m 是 Router2 估计到达路由器 Router1 的延时。若路由器 Router2 知道它到邻居路由器 Router3 的延时为 n，那么它可以得知路由器 Router3 通过 Router2 到达 Router1 需要花费时间 $m+n$。如果路由器 Router3 还有其他相邻路由器，则对于从其他每个邻居那儿收到的距离矢量，该路由器执行同样的计算，最后从中选择费时最小的路由作为路由器 Router3 去往路由器 Router1 的最佳路由，然后更新其路由表，并通告给其邻居路由器。

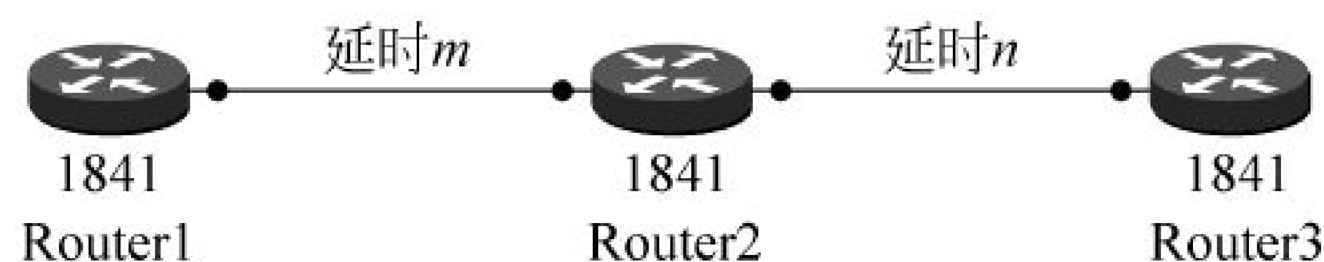


图 6-2 距离矢量路由算法示例

接着，我们再以如图 6-3 所示的更复杂的网络环境为例，介绍距离矢量算法中路由的计算流程，各段链路的延时均已在图中标注。RouterA、RouterB、RouterC、RouterD、RouterE 分别代表 5 个路由器，假设路由表的传递方向为：RouterA→RouterB→RouterC→RouterD→RouterE(这与路由器启动的先后次序有关)。下面介绍路由表的计算过程。

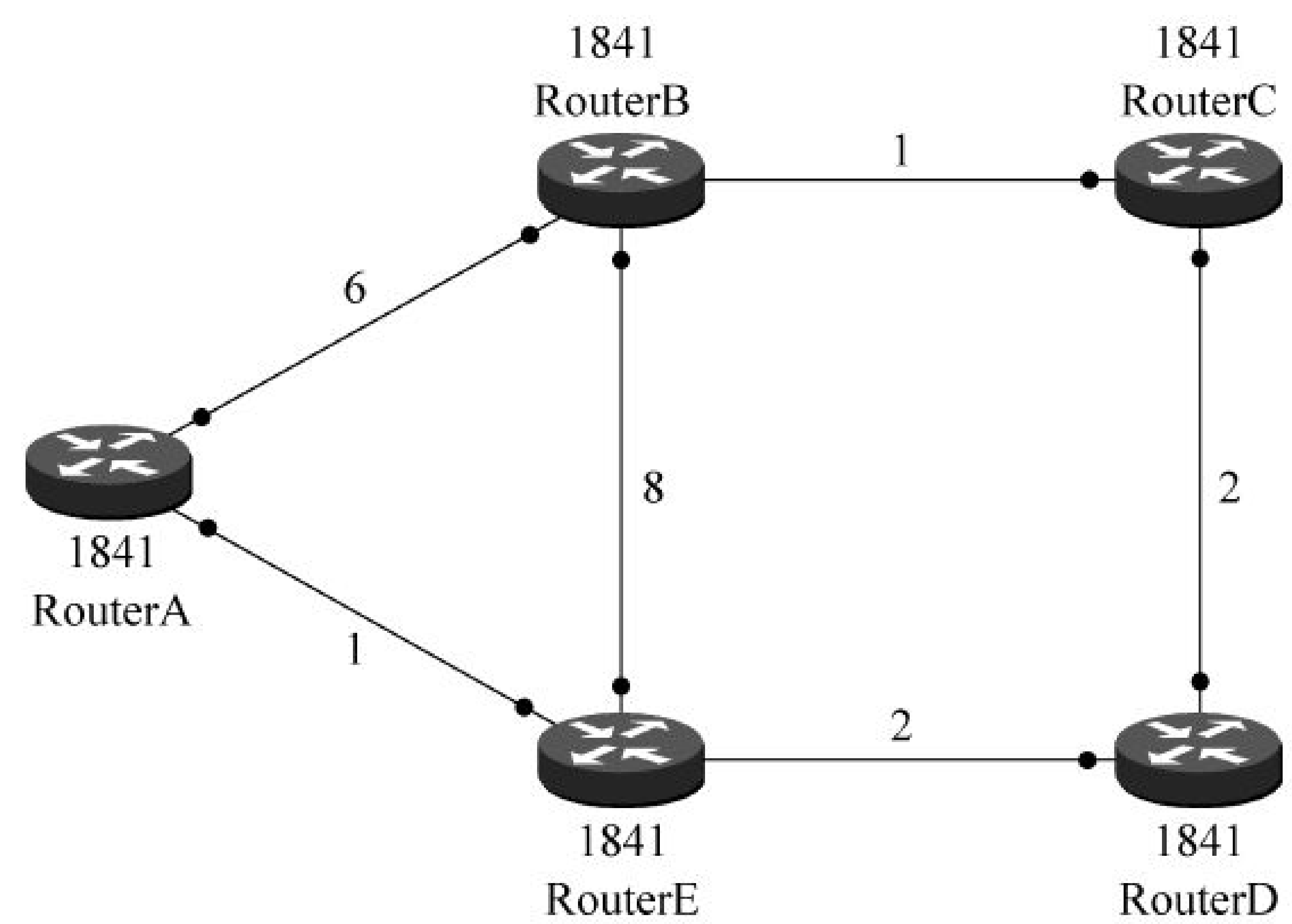


图 6-3　更复杂的距离矢量算法示例

1. 初始路由表

在初始状态下，各路由器都只收集直接相连的链路的延时信息，由路由器拓扑结构得出的初始矢量表见表 6-1～表 6-5。因为各结点间还没有交换路由信息，所以它们的初始状态的路由表与它们的初始矢量表对应。

表 6-1　RouterA 的初始矢量表

目的 源	RouterB	RouterC	RouterD	RouterE
RouterA	6	不直连	不直连	1

表 6-2　RouterB 的初始矢量表

目的 源	RouterA	RouterC	RouterD	RouterE
RouterB	6	1	不直连	8

表 6-3　RouterC 的初始矢量表

目的 源	RouterA	RouterB	RouterD	RouterE
RouterC	不直连	1	2	不直连

表 6-4　RouterD 的初始矢量表

目的 源	RouterA	RouterB	RouterC	RouterE
RouterD	不直连	不直连	2	2

表 6-5　RouterE 的初始矢量表

目的 源	RouterA	RouterB	RouterC	RouterD
RouterE	1	8	不直连	2

2. 路由器 RouterB 形成新的路由表

首先，路由器 RouterA 根据初始矢量表生成的初始路由表，见表 6-6。

表 6-6 路由器 RouterA 根据初始矢量表生成的初始路由表

目的结点	经由结点	最短距离
RouterB		6
RouterE		1

接着，路由器 RouterA 把它的路由表发给路由器 RouterB。路由器 RouterB 会综合从路由器 RouterA 发来的路由表和它自己的初始路由表，更新为一个新的矢量表，最终的矢量表见表 6-7。从表 6-7 中可以看出，从 RouterB 结点到达 RouterE 结点此时存在两条路径：一条是直达的；一条是通过 RouterA 结点到达的。而且这两条线的距离不同，经过 RouterA 结点到达 RouterE 结点的距离(7)比直达线路的距离(8)更短，所以最终在形成的路由表中，把到达 RouterE 结点的线路改为经由 RouterA 结点这条线路，见表 6-8。

表 6-7 路由器 RouterB 的新矢量表

目的结点	经由结点	距离
RouterA		6
RouterC		1
RouterE		8
RouterE	RouterA	7

表 6-8 路由器 RouterB 的最终路由表

目的结点	经由结点	最短距离
RouterA		6
RouterC		1
RouterE	RouterA	7

3. RouterC 形成新的路由表

此时，路由器 RouterB 再把最终形成的路由表发给路由器 RouterC。同样，路由器 RouterC 也要把它原来的初始路由表与从路由器 RouterB 发来的路由表进行综合，形成新的矢量表，最终的矢量表见表 6-9。在新的矢量表中，除了最初的直接连接的 RouterB 和 RouterD 结点间的矢量外，还新收集了到达 RouterA 和 RouterE 结点的矢量信息。因为 RouterC 结点没有与 RouterA 和 RouterE 结点的直接连接，在初始路由表中并没有到达这两个结点的路由信息，所以现在 RouterC 只有采用从路由器 RouterB 发来的路由表中，经过 RouterB 结点到达 RouterA、RouterE 结点的路径。

这里要注意一点，因为在 RouterB 结点路由表中就已识别了直接通过 RouterB 结点到达 RouterE 结点的距离(8)比依次通过 RouterB、RouterA 结点到达 E 结点的距离(7)大，所以在 RouterC 结点路由表中是用依次通过 RouterB、RouterA 结点到达 E 结点这条路径。最终形成的路由表见表 6-10。

表 6-9 路由器 RouterC 的新矢量表

目的结点	经由结点	距离
RouterA	RouterB	7
RouterB		1
RouterD		2
RouterE	RouterB→RouterA	8

表 6-10 路由器 RouterC 的最终路由表

目的结点	经由结点	最短距离
RouterA		7
RouterB		1
RouterD		2
RouterE	RouterB→RouterA	8

4. 路由器 RouterD 形成新的路由表

路由器 Router C 再把它的最终路由表发给路由器 RouterD。同样，路由器 RouterD 也要把它原来的初始路由表与从路由器 RouterC 发来的路由表进行综合，形成新的矢量表，最终的矢量表见表 6-11。在新的矢量表中，除了最初的直接连接的 RouterC 和 RouterE 结点间的矢量信息外，还新收集了到达 RouterA 和 RouterB 结点的矢量信息。因为 RouterD 结点没有与 RouterA 和 RouterB 结点的直接连接，所以在其最初的路由表中并没有到达这两个结点的矢量信息，此时仍采用经过 RouterC 结点到达 RouterA 和 RouterB 结点的路径。

表 6-11 路由器 RouterD 的新矢量表

目的结点	经由结点	距离
RouterA	RouterC	9
RouterB	RouterC	3
RouterC		2
RouterE	RouterC→RouterB→RouterA	10
RouterE		2

在这里同样要注意一点，从 RouterD 结点到达 RouterE 结点也有两条路径：一是直接到达；二是依次通过 RouterC、RouterB、RouterA 结点到达，经过比较发现，直接连接到达的距离(2)比通过 RouterC、RouterB、RouterA 结点到达 E 结点路径的距离(10)要小，所以在 RouterD 结点中，到达 RouterE 结点是采用直接连接这条线路。最终形成的路由表见表 6-12。

表 6-12 路由器 RouterD 的路由表

目的结点	经由结点	最短距离
RouterA	RouterC	9
RouterB	RouterC	3
RouterC		2
RouterE		2

5. 路由器 RouterE 形成新的路由表

路由器 Router D 再把它的最终路由表发给路由器 E。同样，路由器 RouterE 也要把它原来的初始路由表与从 RouterD 路由器发来的路由表进行综合，形成新的矢量表，最终的矢量表见表 6-13。在新的矢量表中，除了最初的直接连接的 RouterA、RouterB 和 RouterD 结点间的矢量外，还新收集了到达 RouterC 结点的矢量信息，因为 RouterE 结点没有与 RouterC 结点的直接连接。此时仍采用经过 RouterD 结点到达 RouterC 结点的路径。

表 6-13 路由器 RouterE 的新矢量表

目的结点	经由结点	距离
RouterA		1
RouterA	RouterD→RouterC→RouterB	11
RouterB		8
RouterB	RouterD→RouterC	5
RouterC	RouterD	4
RouterD		2

在这里有两个要注意的地方：一是从 RouterE 结点到达 RouterA 结点的路径问题，因为此时 RouterE 结点与 RouterA 结点是直接连接的，而且其距离(1)比原来从 RouterD 路由器发来的路由表中提供的通过 RouterD、RouterC、RouterB 结点到达 RouterA 结点路径距离(11)要小，所以在最终的 E 结点路由表中，到达 RouterA 结点是采用直接连接这条线路；二是 RouterE 结点虽然与 B 结点直接连接，但它的距离(8)比原来从 RouterD 路由器发来的路由表中提供的依次经过 RouterD、RouterC 这两个结点到达 B 结点的距离(5)大，所以在最终的 RouterE 结点路由表中，到达 RouterB 结点是采用依次经过 RouterD、RouterC 两个结点这条路径。最终形成的路由表见表 6-14。

表 6-14 路由器 RouterE 的路由表

目的结点	经由结点	最短距离
RouterA		1
RouterB	RouterD→RouterC	5
RouterC	RouterD	4
RouterD		2

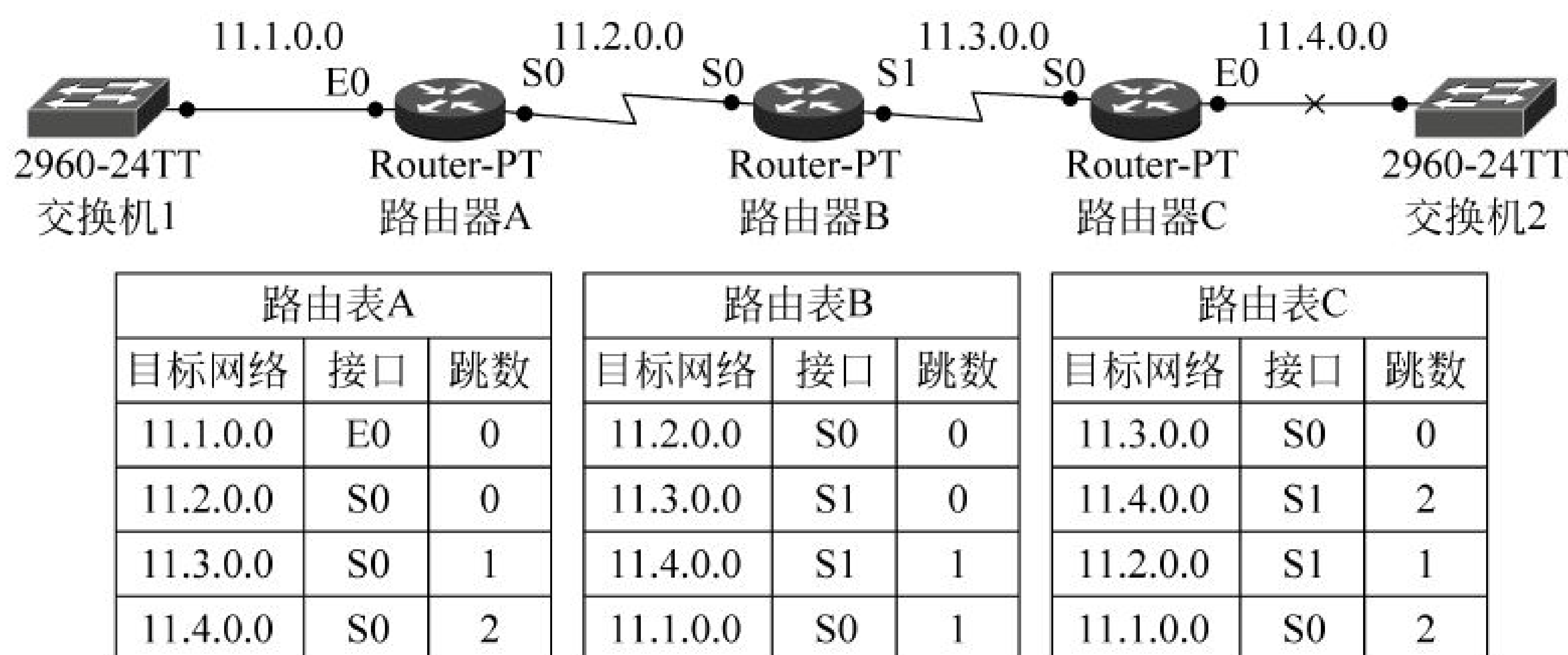
经过以上多个步骤，网络中各路由器就完成了整个路由表的更新。当然，在拓扑结构发生变化时，各路由器的路由表又会发生变化，重新进行更新。

6.4 路由环路及解决方法

路由环路就是数据包不断在这个网络传输，始终到达不了目的地，导致掉线或者网络瘫痪。在维护路由表信息的时候，如果在拓扑发生改变后，网络收敛缓慢产生了不协调或者矛盾的路由选择条目，就会发生路由环路的问题，这种情况下，路由器对无法到达的网络路由不予理睬，导致用户的数据包不停在网络上循环发送，最终造成网络资源的严重浪费。

6.4.1 路由环路产生的原因

路由环路的问题如图 6-4 所示。



路由表A		
目标网络	接口	跳数
11.1.0.0	E0	0
11.2.0.0	S0	0
11.3.0.0	S0	1
11.4.0.0	S0	2

路由表B		
目标网络	接口	跳数
11.2.0.0	S0	0
11.3.0.0	S1	0
11.4.0.0	S1	1
11.1.0.0	S0	1

路由表C		
目标网络	接口	跳数
11.3.0.0	S0	0
11.4.0.0	S1	2
11.2.0.0	S1	1
11.1.0.0	S0	2

图 6-4 路由环路的问题

在网络 11.4.0.0 发生故障之前,所有的路由器都具有正确一致的路由表,网络是收敛的。在本例中,路径开销(即距离)用跳数计算,所以,每条链路的开销是 1。路由器 C 与网络 11.4.0.0 直连,跳数为 0。路由器 B 经过路由器 C 到达网络 11.4.0.0,跳数为 1。路由器 A 经过路由器 B 和路由器 C 到达网络 11.4.0.0,跳数为 2。

如果网络 11.4.0.0 故障,就可能会在路由器之间产生路由环路,下面是产生路由环路的步骤:

(1) 当网络 11.4.0.0 发生故障,路由器 C 最先收到故障信息,路由器 C 把网络 11.4.0.0 设为不可达,并等待更新周期到来通告这一路由变化给相邻路由器。如果路由器 B 的路由更新周期在路由器 C 之前到来,那么路由器 C 就会从路由器 B 那里学习到去往 11.4.0.0 的新路由(实际上,这一路由已经是错误路由了)。这样,路由器 C 的路由表中就记录了一条错误路由(经过路由器 B,可去往网络 11.4.0.0,跳数增加到 2)。

(2) 路由器 C 学习了一条错误信息后,它会把这样的路由信息再次通告给路由器 B,根据通告原则,路由器 B 也会更新这样一条错误路由信息,认为可以通过路由器 C 去往网络 11.4.0.0,跳数增加到 3。

(3) 这样,路由器 B 认为可以通过路由器 C 去往网络 11.4.0.0,路由器 C 认为可以通过路由器 B 去往网络 11.4.0.0,就形成了环路。

6.4.2 路由环路的解决方法

解决路由环路问题的方法主要分为 6 种,即定义最大值、水平分割、路由中毒、反向中毒、控制更新时间和触发更新。

1. 定义最大值

距离矢量路由算法可以通过 IP 头中的生存时间(TTL)自纠错,但路由环路问题可能使跳数值过大,甚至计数到无穷大。为了避免这个问题,距离矢量协议定义了一个跳数最大值,这个跳数最大的度量值为 16。也就是说,路由更新信息最多可以向不可到达的网络的路由中的路由器转发(跳)15 次,一旦达到最大值 16,就视为网络不可到达,存在故障,将不再接收来自访问该网络的任何路由更新信息。

2. 水平分割

水平分割技术可以解决路由环路问题并加快网络收敛。其规则就是不向原始路由更新来的方向再次发送路由更新信息(即仅仅进行单向更新)。例如,有 3 台路由器 A、B、C,B 向 C 学习到访问网络 11.4.0.0 的路径以后,不再向 C 声明自己可以通过 C 访问 11.4.0.0 网络的路径信息,A 向 B 学习到访问 11.4.0.0 网络路径信息后,也不再向 B 声明,而一旦网络 11.4.0.0 发生故障无法访问,C 会向 A 和 B 发送该网络不可达到的路由更新信息,但不会再学习 A 和 B 发送的能够到达 11.4.0.0 的错误信息。

3. 路由中毒

路由中毒也称为路由毒化。定义跳数最大值在一定程度上解决了路由环路问题,但并不彻底,可以看到,在达到最大值之前,路由环路还是存在的。为此,路由中毒就可以彻底解决这个问题。其原理是:假设有 3 台路由器 A、B、C,当网络 11.4.0.0 出现故障无法访问的时候,路由器 C 便向邻居路由发送相关路由更新信息,并将其度量值标为无穷大,告诉它们网络 11.4.0.0 不可到达,路由器 B 收到毒化消息后将该链路路由表项标记为无穷大,表示该路径已经失效,并向邻居 A 路由器通告,依次毒化各个路由器,告诉邻居 11.4.0.0 这个网络已经失效,不再接收更新信息,从而避免了路由环路。

4. 反向中毒

反向中毒也称为毒化逆转。结合上面的例子,当路由器 B 看到到达网络 11.4.0.0 的度量值为无穷大的时候,就发送一个叫作毒化逆转的更新信息给 C 路由器,说明 11.4.0.0 这个网络不可达到,这是超越水平分割的一个特例,这样保证所有的路由器都接收到了毒化的路由信息。

5. 控制更新时间

控制更新时间也称为抑制计时器。抑制计时器用于阻止定期更新的消息在不恰当的时间内重置一个已经失效的路由。抑制计时器告诉路由器把可能影响路由的任何改变暂时保持一段时间,抑制时间通常比更新信息发送到整个网络的时间要长。当路由器从邻居接收到以前能够访问的路由现在不能访问的更新信息后,就将该路由标记为不可访问,并启动一个抑制计时器,如果再次收到从邻居发送来的更新信息,其中包含一个比原来路径具有更小度量值的路由,就标记为可以访问,并取消抑制计时器。如果在抑制计时器超时之前从不同邻居收到的更新信息包含的度量值比以前的更大,更新将被忽略,这样可以有更多的时间让更新信息传遍整个网络。

6. 触发更新

正常情况下,路由器会定期将路由表发送给邻居路由器。而触发更新就是立刻发送路由更新信息,以响应某些变化。检测到网络故障的路由器会立即发送一个更新信息给邻居路由器,并依次产生触发更新通知它们的邻居路由器,使整个网络上的路由器在最短的时间内收到更新信息,从而快速了解整个网络的变化。但这样也会有问题存在,有可能包含更新信息的数据包被网络中的某些链路丢失或损坏,其他路由器没能及时收到触发更新,因此就产生了结合抑制的触发更新。抑制规则要求一旦路由失效,在抑制时间内,到达同一目的地有同样或更差度量值的路由将会被忽略,这样触发更新将有时间传遍整个网络,从而避免了已经损坏的路由重新插入已经收到触发更新的邻居中,也就解决了路由环路的问题。

6.5 RIPv1 报文格式

RIPv1 的报文格式如图 6-5 所示。各字段的长度和解释如下：



图 6-5 RIPv1 的报文格式

(1) 命令(Command)字段，占 8 位。

命令字段用于指定报文的用途。命令有 5 种：Request(请求)、Response(响应)、Traceon(启用跟踪标记，自 RIPv2 起已经淘汰)、Traceoff(关闭跟踪标记，自 RIPv2 起已经淘汰)和 Reserved(保留)。

(2) 版本(Version)字段，占 8 位。

版本字段用于指定 RIP 使用的版本。对于 RIPv1，这个字段的取值必须设置为 1。

(3) 地址类型标识符(Address Family Identifier)字段，占 16 位。

该字段指出入口的协议地址类型。IP 地址的地址类型标识符为 2。由于 RIPv2 版本可能使用几种不同协议传送路由选择信息，所以 RIPv2 要使用到该字段。

(4) 路由标志(Route Tag)字段，占 16 位。

路由标志字段仅在 RIP 第 2 版及第 2 版以上的版本使用。RIPv1 并未使用这个字段，此时必须将这个字段的数值设置为 0。路由标志字段用于路由器指定属性，必须通过路由器保存和重新公告。路由标志是分离内部和外部 RIP 路由线路的一种常用方法(路由选择域内的网络传送线路)，该方法在 EGP 或 IGP 中都有应用。

(5) IP 地址(IP Address)字段，占 32 位。

(6) 子网掩码(Subnet Mask)字段，占 32 位。

子网掩码字段应用于 IP 地址，生成非主机地址部分。如果设置为 0，说明该报文不包括子网掩码。子网掩码字段也仅在 RIPv2 或以上版本使用，对于 RIPv1，并未使用这个字段，此字段必须设置为 0。

（7）下一跳地址（Next Hop）字段，占32位。

下一跳地址字段用于指出下一跳IP地址，由路由入口指定的通向目的地的数据包转发到该地址。对于RIPv1，并未使用这个字段，此字段也必须设置为0。

（8）度量值（Metric）字段，32位。

度量值字段即跳数字段，表示从主机到目的地整个报文传输过程的距离。

6.6 RIP的计时器

RIP通过4个计时器来动态管理和维护路由表。这4个计时器分别是更新计时器、失效计时器、刷新计时器和抑制计时器。

1. 更新计时器

更新计时器的周期为30s，在RIP启动之后，平均每30s更新一次路由。实际上在25.5～30s间的随机数时间更新一次，之所以这样，是为了错峰发送更新，以防止所有路由器同时发送路由更新造成太大流量。启用了RIP的接口会发送自己的除了被水平分割抑制的路由表的完整副本给所有相邻路由器，更新的目标地址为广播地址255.255.255.255。

2. 失效计时器

失效计时器的周期为180s。如果180s（默认值）后还未收到，则刷新现有路由，即将该路由的度量值设置为16，路由表项将被标记为x.x.x.x is possibly down（可能失效）。在刷新计时器超时之前，该路由仍将保留在路由表中。

3. 刷新计时器

刷新计时器的周期为240s。在默认情况下，刷新计时器设置为240s，比失效计时器长60s。当刷新计时器超时后，该路由将从路由表中删除。

4. 抑制计时器

抑制计时器的周期为180s。这个计时器用于稳定路由信息，并有助于在拓扑结构根据新信息收敛的过程中防止路由环路。在某条路由被标记为不可达后，它处于抑制状态的时间必须足够长，以便拓扑结构中的所有路由器能在此期间获知该不可达网络。默认情况下，抑制计时器设置为180s。

RIP的4个计时器的工作原理如图6-6所示。

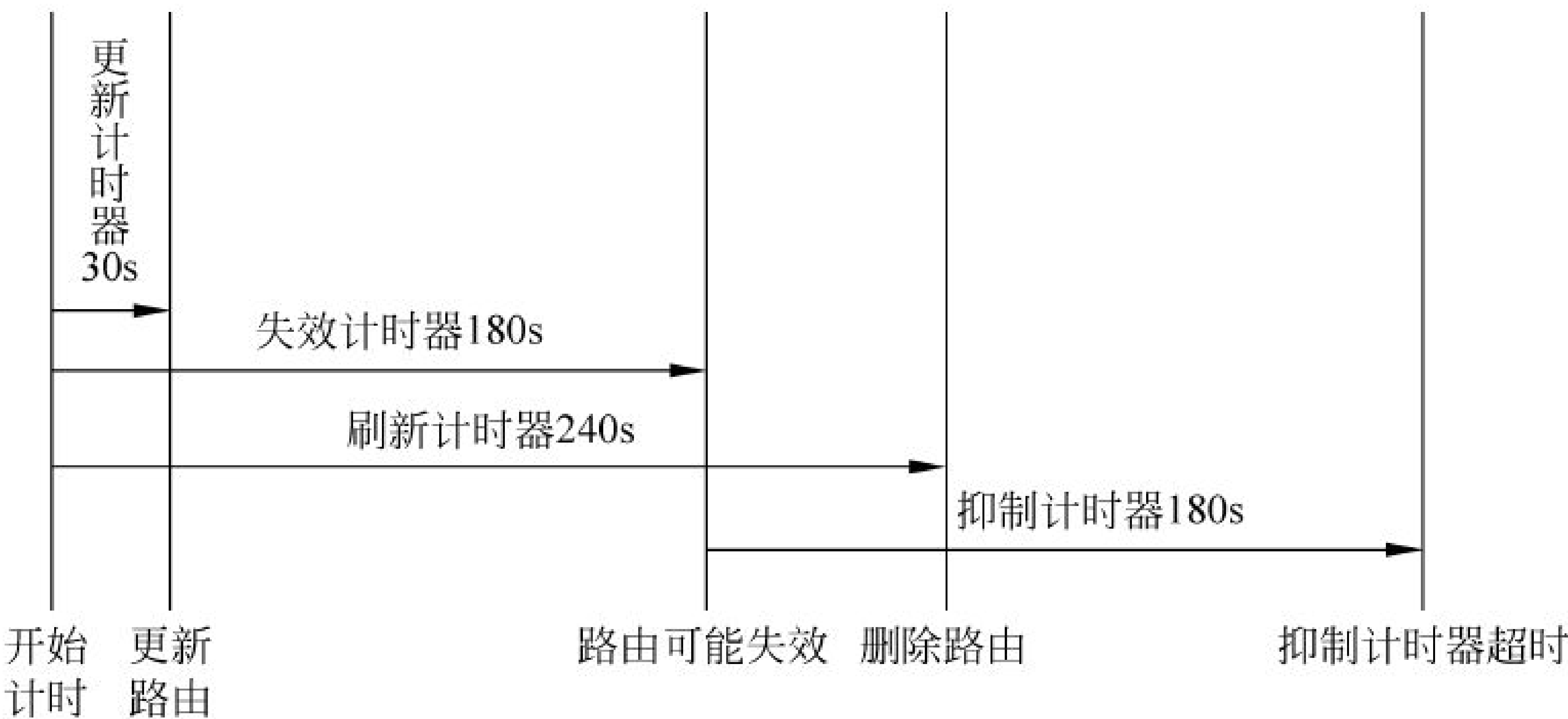


图6-6　RIP的4个计时器的工作原理

一台路由器从接收到邻居发来的路由更新包开始，更新计时器会重置为 0s(秒)并重新计时。RIP 路由器总是每隔 30s 通过 UDP 520 端口以 RIP 广播应答方式向邻居路由器发送一个路由更新包。

如果路由器 30s 还未收到邻居发过来的路由更新包，则更新计时器超时。如果再过 150s，达到 180s(即 30s＋150s＝180s)还没收到路由更新包，则失效计时器超时。然后路由器将邻居路由器的相应路由条目标记为 Possibly down(可能失效)。

当失效计时器计时完成时，立即启动 180s 的抑制计时器。

如果在抑制期间从任何相邻路由器接收到含有更小度量值(跳数更少)的有关该路由条目的更新，则恢复该网络并删除抑制计时器。

如果在抑制期间从相邻路由器收到的更新包含的度量值与之前相同或比之前大，则该更新将被忽略。如此一来，更新信息便可继续在网络中传播一段时间，因为抑制计时器主要用于给路由器一些时间，让网络收敛完成，防止路由环路。所以，收到与原来相同的度量值或更大的度量值的路由更新包将被忽略。

当失效计时器超时，再过 60s，达到 240s 的刷新计时器的终点(180s＋60s＝240s)，还没有收到路由更新包，路由器就刷新路由表，把不可达的路由条目删掉。

当路由器处于抑制周期内，该路由条目依旧用于转发数据。

6.7 RIPv1 的配置与管理

虽然 RIP 的工作原理比较复杂，但是配置却十分简单。下面通过实例来介绍 RIP 第 1 版(RIPv1)的配置和管理方法。

配置和管理 RIPv1 路由的有关命令及其作用解析如下。

```
Router(config)#router rip              启用 RIP 路由协议，进入路由器配置模式。
Router(config)#network 网络地址         为路由器指定已经连接的网络。
Router#show ip route                   查看路由表。
Router#show ip protocols               查看路由协议。
Router#debug ip rip                    实时监控路由器的更新信息。
```

下面以图 6-7 所示的网络环境为例，说明 RIPv1 的配置和管理命令。

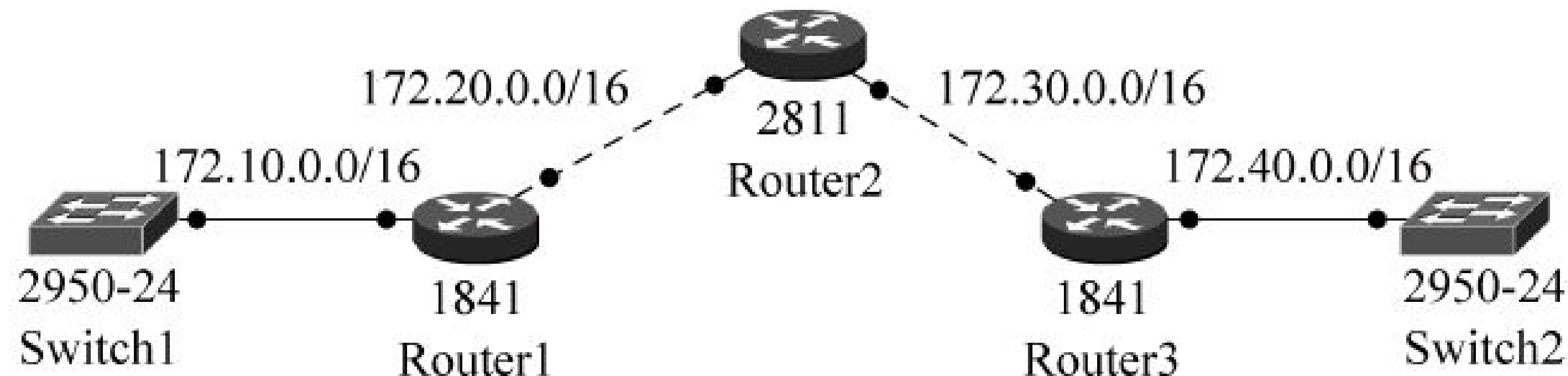


图 6-7 RIPv1 的配置环境

分别在路由器 Router1、路由器 Router2 和路由器 Router3 的全局配置模式下，输入如图 6-8～图 6-10 所示的 RIPv1 配置命令。

接着，可以用 show ip route 查看路由表。路由器 Router1 的路由表如图 6-11 所示。

在图 6-11 中，以字母 R 开头的两行信息表明路由器从邻居处学习到的两条 RIP 路由已经添加到路由表中。去往目标网络地址为 172.30.0.0 的数据包可以经过下一跳为 IP 地

```
Router1(config)#router rip
Router1(config-router)#network 172.10.0.0
Router1(config-router)#network 172.20.0.0
Router1(config-router)#
```

图 6-8　配置路由器 Router1

```
Router2(config)#router rip
Router2(config-router)#network 172.20.0.0
Router2(config-router)#network 172.30.0.0
Router2(config-router)#
```

图 6-9　配置路由器 Router2

```
Router3(config)#router rip
Router3(config-router)#network 172.30.0.0
Router3(config-router)#network 172.40.0.0
Router3(config-router)#
```

图 6-10　配置路由器 Router3

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter are
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.10.0.0/16 is directly connected, FastEthernet0/1
C    172.20.0.0/16 is directly connected, FastEthernet0/0
R    172.30.0.0/16 [120/1] via 172.20.0.2, 00:00:15, FastEthernet0/0
R    172.40.0.0/16 [120/2] via 172.20.0.2, 00:00:15, FastEthernet0/0
Router1#
```

图 6-11　路由器 Router1 的路由表

址 172.20.0.2 的路由送出；而去往目标网络地址为 172.40.0.0 的数据包可以经过下一跳为 IP 地址 172.20.0.2 的路由送出。

由于网络收敛需要一定的时间(更新周期约为 30s)，因此执行配置命令后，如果立即用 show ip route 命令查看配置结果，以字母 R 开头的动态路由信息也许不会立即显示出来。此时，请耐心等候一下，并检查输入的配置命令是否正确。一旦所有路由器上的路由信息都得到正确配置，则 show ip route 命令将会反映出当前路由器的完整的路由表。

也可以用 show ip protocols 命令查看路由器当前使用的路由协议。这个命令可以显示路由协议的详细信息，从而检验路由器的工作情况。在本例中，路由器 Router1 的路由协议信息如图 6-12 所示。

从图 6-12 中的第 2～4 行可以看出，当前配置的路由协议是 RIP；路由更新信息每隔 30s 发送一次，路由更新信息下一次的发送时间是 17s 以后；失效计时器参数为 180s，抑制计时器参数为 180s，刷新计时器参数为 240s。

从图 6-12 中的第 8～11 行可以看出，当前配置的路由协议发送数据支持 RIP 第 1 版的数据包，接收数据支持任何版本，即可以同时接收第 1 版和第 2 版的 RIP 数据包。

```
1  Router1#show ip protocols
2  Routing Protocol is "rip"
3  Sending updates every 30 seconds, next due in 17 seconds
4  Invalid after 180 seconds, hold down 180, flushed after 240
5  Outgoing update filter list for all interfaces is not set
6  Incoming update filter list for all interfaces is not set
7  Redistributing: rip
8  Default version control: send version 1, receive any version
9    Interface              Send  Recv  Triggered RIP  Key-chain
10   FastEthernet0/1        1     2 1
11   FastEthernet0/0        1     2 1
12 Automatic network summarization is in effect
13 Maximum path: 4
14 Routing for Networks:
15         172.10.0.0
16         172.20.0.0
17 Passive Interface(s):
18 Routing Information Sources:
19         Gateway          Distance      Last Update
20         172.20.0.2            120      00:00:21
21 Distance: (default is 120)
22 Router1#
```

图 6-12　路由器 Router1 的路由协议信息

从图 6-12 中的第 12 行可以看出，当前配置的路由协议自动汇总功能已经生效。

从图 6-12 中的第 13 行可以看出，当前配置的路由协议支持最多 4 条等价路由，来实现网络数据流量的负载均衡。

从图 6-12 中的第 14～16 行可以看出，当前已经为路由器指定的网络为 172.10.0.0 和 172.20.0.0，即关注来自网络 172.10.0.0 和 172.20.0.0 的数据包。

从图 6-12 中的第 17 行可以看出，当前路由器的工作模式为被动接口模式。

从图 6-12 中的第 18～21 行可以看出，当前路由信息的来源（即路由器的邻居）为 172.20.0.2，网关为 172.20.0.2，管理距离值为 120，路由信息最近一次的更新时间为 21s 之前。

除了以上测试命令外，还可以用 debug ip rip 命令实时监控路由器的更新信息的情况。

debug 命令是一个用来诊断和发现网络问题的实用工具，提供了实时和持续的信息。由于在 CPU 中 debug 命令的输出被分配了很高的优先级，因此这个命令有可能导致系统瘫痪。基于这个原因，建议只在对某个特定问题查错时，才使用 debug 命令。

例如，在路由器 Router1 的特权模式下，用 debug ip rip 命令可以得到如图 6-13 所示的测试结果。

图 6-13 中的第 3 行表示收到来自 172.20.0.2 的快速以太网接口 0/0 的格式为 RIPv1 的更新路由信息。第 4 行表示经过 1 跳可以到达网络 172.30.0.0，第 5 行表示经过 2 跳可以到达网络 172.40.0.0。

图 6-13 中的第 6 行表示路由器向广播地址 255.255.255.255 发送格式为 RIPv1 的更新路由表信息。

图 6-13 中的第 7～10 行表示更新路由表，其中包括 3 条路由，到达网络 172.20.0.0 的跳数为 1，到达网络 172.30.0.0 的跳数为 2，到达网络 172.40.0.0 的跳数为 3。

图 6-13 中的第 11 行表示路由器向广播地址 255.255.255.255 发送格式为 RIPv1 的更新路由表信息。

```
1  Router1#debug ip rip
2  RIP protocol debugging is on
3  Router1#RIP: received v1 update from 172.20.0.2 on FastEthernet0/0
4        172.30.0.0 in 1 hops
5        172.40.0.0 in 2 hops
6  RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/1 (172.
7  RIP: build update entries
8        network 172.20.0.0 metric 1
9        network 172.30.0.0 metric 2
10       network 172.40.0.0 metric 3
11 RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (172.
12 RIP: build update entries
13       network 172.10.0.0 metric 1
14 RIP: received v1 update from 172.20.0.2 on FastEthernet0/0
15       172.30.0.0 in 1 hops
16       172.40.0.0 in 2 hops
17 RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/1 (172.
18 RIP: build update entries
19       network 172.20.0.0 metric 1
20       network 172.30.0.0 metric 2
21       network 172.40.0.0 metric 3
22 RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (172.
23 RIP: build update entries
24       network 172.10.0.0 metric 1
```

图 6-13 用 debug ip rip 命令实时监控路由器的更新信息

如果再等待 30s，将会发现图 6-13 所示的信息又会重复出现，这是因为 RIP 每 30s 就会发送定期更新信息。

如果要停止路由器上的监控信息，请输入 no debug ip rip 命令。

通过执行以上介绍的 show ip route 命令、show ip protocols 命令和 debug ip rip 命令，可以确认路由器 Router1 上的 RIP 协议工作完全正常。

6.8 RIPv2 的配置与管理

6.8.1 RIPv1 与 RIPv2 的特性比较

RIPv1 与 RIPv2 的特性比较见表 6-15。RIPv2 的数据包格式如图 6-14 所示。

表 6-15 RIPv1 与 RIPv2 的特性比较

特 性	RIPv1	RIPv2
采用跳数为度量值	是	是
15 是最大的有效度量值，16 为无穷大	是	是
默认更新周期为 30s	是	是
周期更新时发送全部路由信息	是	是
拓扑改变时发送只针对变化的触发更新	是	是
使用水平分割、路由毒化、毒性逆转	是	是
使用抑制计时器	是	是
发送更新的方式	广播	组播
使用 UDP520 端口发送报文	是	是
更新中携带子网掩码，支持 VLSM	否	是
支持认证	否	是



图 6-14 RIPv2 的数据包格式

与 RIPv1 相比，RIPv2 拥有以下扩展特性。

(1) 支持子网掩码，RIPv2 每个路由条目都携带自己的子网掩码。

(2) RIPv2 可以对路由更新信息进行认证，以避免攻击者将未知的路由设备悄无声息地加入网络中。

(3) RIPv2 每个路由条目都携带下一跳地址。

(4) RIPv2 放弃广播更新的方式，而是通过组播的方式发送更新，更新消息的目的地址变为 224.0.0.9。这样可以避免无关路由器查看 RIP 信息，浪费设备资源。

(5) RIPv2 对数据包的格式也作了补充，与 RIPv1 相比，RIPv2 数据包的格式增加了路由标志、子网掩码和下一跳地址等字段。

6.8.2 RIPv2 的配置与管理

配置 RIPv2 的方法与配置 RIPv1 很相似，只增加一条指定版本的命令 version 2 即可。RIPv1 原来的配置命令对于 RIPv2 仍然有效。RIPv2 的配置相关命令如下。

```
Router(config)#router rip              启用 RIP 路由器，进入路由器配置模式。
Router(config)#network 网络地址        为路由器指定已经连接的网络。
Router#show ip route                   查看路由表。
Router#show ip protocols               查看路由协议。
Router#debug ip rip                    实时监控路由器的更新信息。
Router(config)#version 1 或 2          指定发送和接收数据包的版本号。
Router(config)#no autosummary          关闭自动汇总功能。
```

RIPv1 属于有类的距离矢量路由协议，不支持子网掩码；而 RIPv2 属于无类的距离矢量路由协议，支持子网掩码，因此，RIPv2 配置时需要关闭自动汇总功能。

下面以图 6-15 所示的网络环境为例，介绍 RIPv2 的配置方法。

首先，在路由器 Router1 的全局配置模式上进行基本接口配置，如图 6-16 所示。

接着，在路由器 Router2 的全局配置模式上进行基本接口配置，如图 6-17 所示。

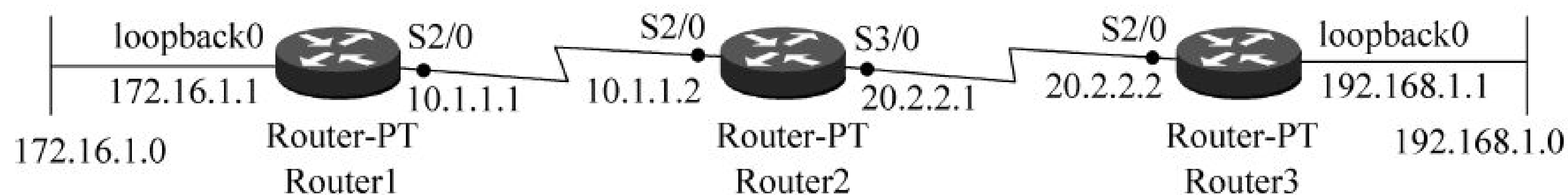


图 6-15　RIPv2 配置示例的网络环境

```
Router1(config)#interface Serial 2/0
Router1(config-if)#ip address 10.1.1.1 255.255.255.0
Router1(config-if)#clock rate 128000
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface loopback 0
Router1(config-if)#ip address 172.16.1.1 255.255.255.0
Router1(config-if)#
```

图 6-16　路由器 Router1 的基本接口配置

```
Router2(config)#interface serial 2/0
Router2(config-if)#ip address 10.1.1.2 255.255.255.0
Router2(config-if)#clock rate 128000
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface serial 3/0
Router2(config-if)#ip address 20.2.2.1 255.255.255.0
Router2(config-if)#clock rate 128000
Router2(config-if)#no shutdown
Router2(config-if)#
```

图 6-17　路由器 Router2 的基本接口配置

同理，在路由器 Router3 的全局配置模式上进行基本接口配置，如图 6-18 所示。

```
Router3(config)#interface serial 2/0
Router3(config-if)#ip address 20.2.2.2 255.255.255.0
Router3(config-if)#clock rate 128000
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#interface loopback 0

%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
Router3(config-if)#ip address 192.168.1.1 255.255.255.0
Router3(config-if)#
```

图 6-18　路由器 Router3 的基本接口配置

下一步是本例配置的重点，即通过动态路由协议 RIPv2 实现各个网段之间的通信，在路由器 Router1 的全局配置模式上进行 RIPv2 配置，具体操作命令如图 6-19 所示。

```
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#no auto-summary
Router1(config-router)#network 172.16.0.0
Router1(config-router)#network 10.0.0.0
Router1(config-router)#
```

图 6-19　路由器 Router1 的 RIPv2 配置

接着，对路由器 Router2 进行 RIPv2 配置，具体操作命令如图 6-20 所示。

```
Router2(config)#router rip
Router2(config-router)#version 2
Router2(config-router)#no auto-summary
Router2(config-router)#network 10.0.0.0
Router2(config-router)#network 20.0.0.0
Router2(config-router)#
```

图 6-20 路由器 Router2 的 RIPv2 配置

同理，对路由器 Router3 进行 RIPv2 配置，具体操作命令如图 6-21 所示。

```
Router3(config)#router rip
Router3(config-router)#version 2
Router3(config-router)#no auto-summary
Router3(config-router)#network 20.0.0.0
Router3(config-router)#network 192.168.1.0
Router3(config-router)#
```

图 6-21 路由器 Router3 的 RIPv2 配置

至此，如果上述每个路由器的每条配置命令都正确输入的话，各路由器就可以通过 RIPv2 动态路由协议实现网络通信，即 RIPv2 配置成功了。

配置成功之后，可以使用命令 show ip protocols 显示当前使用的动态路由协议、路由器的更新时间、在当前协议中连接的网络、管理距离等详细信息，如图 6-22 所示。

```
Router1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 21 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial2/0             2     2
  Loopback0             2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        172.16.0.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
        10.1.1.2             120      00:00:17
Distance: (default is 120)
Router1#
```

图 6-22 查看路由器 Router1 的路由协议信息

此时，我们也可以在路由器 Router1 上用命令 ping 测试与路由器 Router3 的接口 192.168.1.1 的连通性，结果如图 6-23 所示，表明网络连接正常。

```
Router1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 s
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4

Router1#
```

图 6-23 测试网络的连通性

6.9 RIPng的配置与管理

6.9.1 RIPng的工作原理

IETF在1997年为了解决RIP与IPv6的兼容性问题，对RIP协议进行了改进，制定了基于IPv6的RIPng(RIP next generation)协议，定义在RFC2080中。

RIPng的度量也是基于跳数的，每经过一台路由器，路径的跳数加1。因此，跳数越多，路径越长，路由算法会优先选择跳数少的路径。RIPng支持的最大跳数是15，跳数为16的网络被认为不可达。

RIPng中路由的更新是通过定时广播的实现的。每个路由表有一个更新计时器(Update Timer)，默认情况下，路由器每隔30s向与它相连的网络广播自己的路由表，接到广播的路由器将收到的信息添加至自身的路由表中。每个路由器都如此广播，最终网络上所有的路由器都会得知全部的路由信息。正常情况下，每30s路由器就可以收到一次路由信息确认，如果经过180s，即6个更新周期，某个路由条目仍然没有得到确认，路由器就认为它已失效了。如果再经过120s，路由条目还是没有得到确认，它就被从路由表中删除。这里的30s、180s和120s的延时都是由定时器控制的。定时器在RIPng中起着非常重要的作用，RIPng使用定时器来实现路由表的更新、报文的发送。周期性的报文广播是由定时器实现的。另外，为防止路由表长时间未更新而失效，每个路由条目有两个定时器与之联系，超时的路由条目最终将会被删除，以防止路由器广播和使用已经失效的路由。RIPng的定时器有3个，即更新定时器、期满定时器和垃圾收集定时器。

1. 更新定时器

此定时器被设置成25～35s之间的任一随机数。这样设置的目的是为了避免网络上所有路由器以相同的定时发送更新报文，利用随机间隔可以均衡通信量，从而减少路由器之间发生冲突的可能性。

2. 期满定时器

路由器只要收到通往特定信宿路由，就对通往该信宿的期满定时器初始化。期满定时器被设定为180s，如果一条路由在期满定时器超时前未得到相关报文的更新，则该条路由不再有效，但仍保留在路由表中，以便通知其他路由器这条路由已经失效。

3. 垃圾收集定时器

路由器对无效路由加上跳数为无穷大的无效标记并将垃圾收集定时器初始化。此时，垃圾收集定时器被设置为120s，在这段时间内这些路由仍然会被路由器周期性地广播，这样相邻路由器就能及时地从路由表中删除该路由。

RIPng的报文格式如图6-24所示。

RIPng协议用UDP(用户数据报协议)进行传输，使用端口号521发送和接收数据报。RIPng报文分为两类：选路信息报文和用于请求信息的报文。它们都使用相同格式，由固定的首部和路由条目(Route Table Entry，RTE)组成，其中路由条目可以有多个。

RIPng报文首部包括命令字段和版本号字段。同RIP一样，命令字段用来区分报文要实现的各种操作。其中，命令字段取值为1时表示请求部分或全部路由的信息，命令字段取值为2时表示响应。



图 6-24 RIPng 的报文格式

RIPng 路由条目的格式如图 6-25 所示。每个路由条目包括前缀(16B)、路由标记(2B)、前缀长度(1B)和度量值(1B)等。



图 6-25 RIPng 路由条目的格式

6.9.2 RIPng 与 RIPv1、RIPv2 的比较

根据以上介绍，可以看到 RIPng 的目标并不是创造一个全新的协议，而是对 RIP 进行必要的改造，以使其适应 IPv6 下的选路要求。因此，RIPng 的基本工作原理同 RIP 一样，其主要变化在地址和报文格式方面。下面列举了一些 RIPv1、RIPv2 与 RIPng 之间的主要区别。

1. 地址版本

RIPv1、RIPv2 是基于 IPv4 的，地址字段长度只有 32b，而 RIPng 基于 IPv6，使用的所有地址长度均为 128b。

2. 子网掩码和前缀长度

RIPv1 被设计成用于无子网的网络，因此没有子网掩码的概念，这就决定了 RIPv1 不能用于传播变长的子网地址或用于 CIDR(无类别域间路由)的无类型地址。RIPv2 增加了对子网选路的支持，因此使用子网掩码区分网络路由和子网路由。IPv6 的地址前缀有明确的含义，因此 RIPng 中不再有子网掩码的概念，取而代之的是前缀长度。同样，由于使用了 IPv6 地址，RIPng 中也没有必要再区分网络路由、子网路由和主机路由。

3. 协议的使用范围

RIPv1、RIPv2 的使用范围被设计成不只局限于 TCP/IP 协议簇，还能适应其他网络协议簇的规定。因此，报文的路由条目中包含有网络协议簇字段，但实际的应用环境很少被用于其他非 IP 的网络，因此 RIPng 中去掉了对这一功能的支持。

4. 对下一跳的表示

RIPv1 中没有下一跳的信息，接收端路由器把报文的源 IP 地址作为到目的网络路由的下一跳。RIPv2 中明确包含了下一跳信息，便于选择最优路由和防止出现选路环路及慢收敛。与 RIPv2 不同，为防止 RTE 过长，同时也为提高路由信息的传输效率，RIPng 中的下一跳字段是作为一个单独的 RTE 存在的。

5. 报文长度

RIPv1、RIPv2 中对报文的长度均有限制，规定每个报文最多只能携带 25 个 RTE。而 RIPng 对报文长度、RTE 的数目都不作规定，报文的长度是由介质的 MTU(最大传输单元)决定的。RIPng 对报文长度的处理，提高了网络对路由信息的传输效率。

6. 广播与组播

RIPv1 使用广播方式发送路由表更新信息。RIPv2 通过组播的方式发送更新，更新消息的目的地址变为 224.0.0.9。而 RIPng 则使用 FF02::9 这个地址进行组播更新。

6.9.3 RIPng 配置与管理

配置 RIPng 协议需要做以下 4 个方面的工作：

(1) 全局启用转发 IPv6 单播特性。

(2) 启用 RIPng 进程。每台路由器上可以启用多个进程，每个启程用不同名字区分。

(3) 在接口模式上，将接口运行在 RIPng 进程中。

(4) 其他优化配置。例如，调整计时器、过滤路由、路由重分布等。

RIPng 协议常用的配置命令格式及解释如下：

```
ipv6 unicast - routing                     全局启用转发 IPv6 单播特性。
ipv6 router rip 进程名称                   启用进程。
ipv6 rip 进程名称 enable                   将接口运行在 RIPng 进程中。
ipv6 enable                                在接口上激活 IPv6 进程。
maximum - paths 最大等值路径条数            设置最大等值路径条数，最大为 64，默认为 4。
ipv6 rip 名字 default - information        创建指定名字的默认路由。
```

下面以图 6-26 所示的 IPv6 网络环境为例，介绍 RIPng 动态路由协议的配置方法。

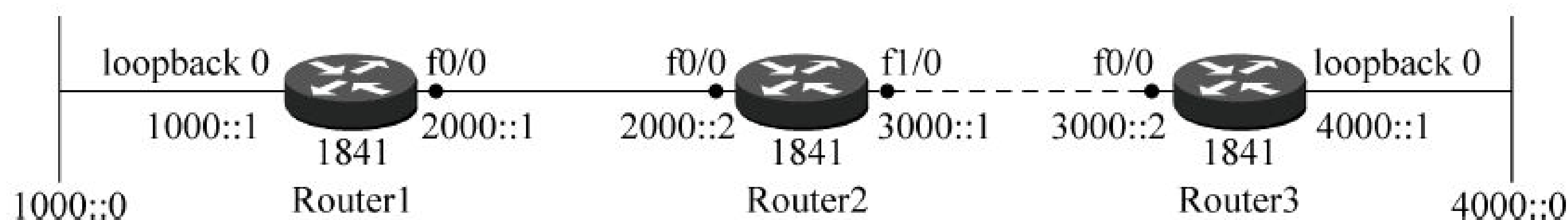


图 6-26 RIPng 的配置环境

第一步，对路由器 Router1 进行配置，具体的配置命令及结果如图 6-27 所示。

其中，第 1 行命令的作用是全局启用转发 IPv6 单播特性；第 2 行命令是启用名称为 demo 的进程；紧接着的命令是为环回接口配置 IPv6 地址 1000::1/64，将接口运行在名称为 demo 的进程中，并激活进程和接口；最后是为接口 FastEthernet0/0 配置 IPv6 地址 2000::1/64，将接口运行在名称为 demo 的进程中，并激活进程和接口。

第二步，对路由器 Router2 进行配置，具体的配置命令及结果如图 6-28 所示。其中，第 1 行命令的作用是全局启用转发 IPv6 单播特性；第 2 行命令是启用名称为 demo 的进程；

```
Router1(config)#ipv6 unicast-routing
Router1(config)#ipv6 router rip demo
Router1(config-rtr)#exit
Router1(config)#interface loopback 0

%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
Router1(config-if)#ipv6 address 1000::1/64
Router1(config-if)#ipv6 rip demo enable
Router1(config-if)#exit
Router1(config)#interface FastEthernet 0/0
Router1(config-if)#ipv6 rip demo enable
Router1(config-if)#ipv6 enable
Router1(config-if)#ipv6 address 2000::1/64
Router1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state t
Router1(config-if)#
```

图 6-27 路由器 Router1 的 RIPng 协议配置

紧接着的命令是为接口 FastEthernet0/0 配置 IPv6 地址 2000::2/64，将接口运行在名称为 demo 的进程中，并激活进程和接口；然后是为接口 FastEthernet0/1 配置 IPv6 地址 3000::1/64，将接口运行在名称为 demo 的进程中，并激活进程和接口。

```
Router2(config)#ipv6 unicast-routing
Router2(config)#ipv6 router rip demo
Router2(config-rtr)#exit
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ipv6 address 2000::2/64
Router2(config-if)#ipv6 rip demo enable
Router2(config-if)#ipv6 enable
Router2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state t
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
o up
Router2(config-if)#exit
Router2(config)#interface fastethernet 0/1
Router2(config-if)#ipv6 address 3000::1/64
Router2(config-if)#ipv6 rip demo enable
Router2(config-if)#ipv6 enable
Router2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state t
Router2(config-if)#
```

图 6-28 Router2 的 RIPng 协议配置

第三步，对路由器 Router3 进行配置，具体的配置命令及结果如图 6-29 所示。

至此，RIPng 协议配置完成，可用 show ipv6 route 查看路由表，如图 6-30 所示。

同理，也可以用 ping 命令测试 IPv6 网络的连通性，结果如图 6-31 所示。

从图 6-31 中可以看到，从路由器 Router1 可以 ping 通路由器 Router3 的 IPv6 地址 4000::1，表明网络连接正常，即基于 RIPng 动态协议的 IPv6 网络配置成功。

```
Router3(config)#ipv6 unicast-routing
Router3(config)#ipv6 router rip demo
Router3(config-rtr)#exit
Router3(config)#interface FastEthernet 0/0
Router3(config-if)#ipv6 address 3000::2/64
Router3(config-if)#ipv6 rip demo enable
Router3(config-if)#ipv6 enable
Router3(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state t
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
o up
Router3(config-if)#exit
Router3(config)#interface loopback 0

%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
Router3(config-if)#ipv6 address 4000::1/64
Router3(config-if)#ipv6 rip demo enable
Router3(config-if)#ipv6 enable
Router3(config-if)#
```

图 6-29 Router3 的 RIPng 协议配置

```
Router1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - E
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, C
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   1000::/64 [0/0]
     via ::, Loopback0
L   1000::1/128 [0/0]
     via ::, Loopback0
C   2000::/64 [0/0]
     via ::, FastEthernet0/0
L   2000::1/128 [0/0]
     via ::, FastEthernet0/0
R   3000::/64 [120/1]
     via FE80::230:A3FF:FEC4:B901, FastEthernet0/0
R   4000::/64 [120/2]
     via FE80::230:A3FF:FEC4:B901, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
Router1#
```

图 6-30 查看路由器 Router1 的 IPv6 路由表

```
Router1#ping 4000::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4000::1, timeout is 2 sec
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#
```

图 6-31 用 ping 命令测试 IPv6 网络的连通性

6.10 本章总结

路由信息协议(Routing Information Protocol,RIP)是应用较早、使用较普遍的内部网关协议(Interior Gateway Protocol,IGP),适用于小型同类网络的一个自治系统(AS)内的路由信息的传递。RIP 是基于距离矢量算法(Distance Vector Algorithms,DVA)的。它使用"跳数",即 metric 作为度量值来衡量到达目标地址的路由距离。目前,RIP 的最新版本是 RIPng,支持 IPv6 协议。

Charles Hedrick 在 1988 年编写了 RFC 1058,他在该文档中阐述了现有的 RIP 并进行了一些改进。从那时开始,RIP 逐步完善,1994 年开发了 RIPv2 协议,到了 1997 年,支持 IPv6 的 RIPng 协议正式问世。

RIP 用"路程段数"(即"跳数")作为网络距离的尺度。每个路由器在给相邻路由器发出路由信息时,都会给每个路径加上内部距离。

距离矢量路由协议共有 3 种,分别是 RIP、IGRP 和 EIGRP。

距离矢量路由算法的基本思想如下:每个路由器维护一个距离矢量(通常是用延时的长短来计算的)表,然后通过相邻路由器之间的距离矢量通告进行距离矢量表的更新。每个距离矢量表项包括两部分:到达目的结点的最佳输出线路;到达目的结点所需时间或距离。通信子网中的其他每个路由器在表中占据一个表项,并作为该表项的索引。每隔一段时间,路由器会向所有邻居结点发送它到每个目的结点的距离表,同时它也接收每个邻居结点发来的距离表。以此类推,经过一段时间后便可将网络中各路由器获得的距离矢量信息在各路由器上统一起来,这样各路由器只需要查看这个距离矢量表,就可以为不同来源分组找到一条最佳的路由。

任何距离矢量路由选择协议(如 RIP)都存在这样一个问题,即路由器并不了解整个网络的情况,因此路由器必须依靠相邻路由器获取网络的可达信息。由于路由选择更新信息在网络上传播慢,距离矢量路由选择算法有一个慢收敛问题,这个问题将导致不一致性产生。RIP 使用计数到无穷大、水平分割法、有破坏逆转的水平分割法、保持定时器法和触发更新法等机制减少因网络上的不一致带来的路由选择环路的可能性。

RIPv1 报文格式包括命令、版本、地址类型标识符、路由标志、IP 地址、子网掩码、下一跳地址和度量等字段。

RIP 协议通过 4 个计时器来动态地管理和维护路由表。这 4 个计时器分别是更新计时器、失效计时器、刷新计时器和抑制计时器。

配置和管理 RIPv1 路由的有关命令及其作用解析如下。

```
Router(config)# router rip              启用 RIP 路由器,进入路由器配置模式。
Router(config)# network 网络地址         为路由器指定已经连接的网络。
Router# show ip route                   查看路由表。
Router# show ip protocols               查看路由协议。
Router# debug ip rip                    实时监控路由器的更新信息。
```

与 RIPv1 相比,RIPv2 拥有以下扩展特性。

(1) 支持子网掩码,每个路由条目都携带自己的子网掩码。

(2) 可以对路由更新信息进行认证,以避免攻击者将未知的路由设备悄无声息地加入网络中。

(3) 每个路由条目都携带下一跳地址。

(4) 放弃广播更新的方式,而是通过组播的方式发送更新,更新消息的目的地址变为224.0.0.9。这样可以避免无关路由器查看RIP信息,浪费设备资源。

(5) RIPv2对数据包的格式也作了补充。RIPv2的数据包格式如图6-14所示。与RIPv1相比,RIPv2的数据包格式增加了路由标志、子网掩码和下一跳地址等字段。

配置RIPv2的方法与配置RIPv1很相似,只增加一条指定版本的命令version 2即可。RIPv1原来的配置命令对于RIPv2仍然有效。RIPv2的配置相关命令如下。

```
Router(config)#router rip              启用RIP路由器,进入路由器配置模式。
Router(config)#network 网络地址         为路由器指定已经连接的网络。
Router#show ip route                   查看路由表。
Router#show ip protocols               查看路由协议。
Router#debug ip rip                    实时监控路由器的更新信息。
Router(config)#version 1 或 2          指定发送和接收数据包的版本号。
Router(config)#no autosummary          关闭自动汇总功能。
```

RIPv1属于有类的距离矢量路由协议,不支持子网掩码;而RIPv2属于无类的距离矢量路由协议,支持子网掩码,因此,RIPv2配置时需要关闭自动汇总功能。

RIPng中路由的更新是通过定时广播实现每个路由表有一个更新计时器(Update Timer),默认情况下,路由器每隔30s向与它相连的网络广播自己的路由表,接到广播的路由器将收到的信息添加至自身的路由表中。每个路由器都如此广播,最终网络上所有的路由器都会得知全部的路由信息。

RIPng协议用UDP(用户数据报协议)进行传输,使用端口号521发送和接收数据报。RIPng报文分为两类:选路信息报文和用于请求信息的报文。它们都使用相同格式,由固定的首部和路由条目(Route Table Entry,RTE)组成,其中路由条目可以有多个。

RIPng协议常用的配置命令格式及解释如下:

```
ipv6 unicast-routing                     全局启用转发IPv6单播特性。
ipv6 router rip 进程名称                 启用进程。
ipv6 rip 进程名称 enable                 将接口运行在RIPng进程中。
ipv6 enable                              在接口上激活IPv6进程。
maximum-paths 最大等值路径条数            设置最大等值路径条数,最大为64,默认为4。
ipv6 rip 名字 default-information        创建指定名字的默认路由。
```

复习思考题

1. 请简述RIP的发展史。
2. 请画图说明RIP的工作原理。
3. 请说明RIP通过哪些方法解决收敛慢的问题。
4. 请画图说明RIPv1的报文格式。
5. RIP包括哪些计时器?每个计时器的功能是什么?

6. 请说明配置和管理 RIPv1 的相关命令。
7. 与 RIPv1 相比，RIPv2 有什么特性？
8. 请说明配置和管理 RIPv2 的相关命令。
9. 请说明 RIPng 的工作原理。
10. RIPng 与 RIPv1、RIPv2 有什么区别？
11. 请说明配置和管理 RIPng 的相关命令。
12. 实训操作题 1：请按图 6-32 所示的网络环境配置 RIPv1 协议。

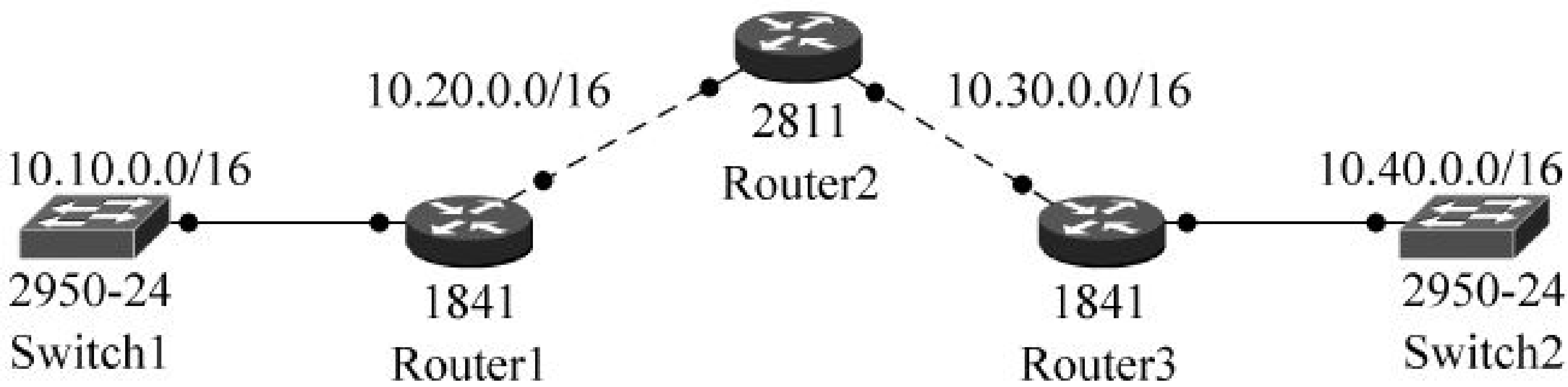


图 6-32　实训操作题 1 的网络环境

13. 实训操作题 2：请按图 6-33 所示的网络环境配置 RIPv2 协议。

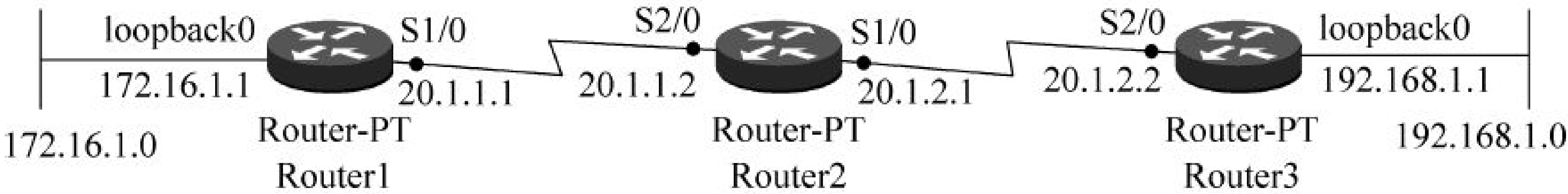


图 6-33　实训操作题 2 的网络环境

14. 实训操作题 3：请按图 6-34 所示的网络环境配置 RIPng 协议。

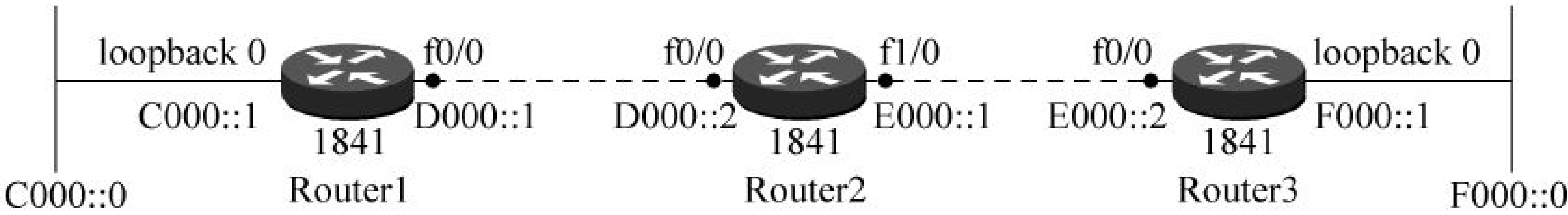


图 6-34　实训操作题 3 的网络环境

第 7 章 OSPF 协议

CHAPTER 7

开放最短路径优先(Open Shortest Path First,OSPF)协议是一种内部网关协议(Interior Gateway Protocol,IGP)。“开放”指的是非私有的,即对公众开放,各个厂商都能兼容 OSPF 协议。OSPF 采用链路状态路由选择算法,用于在单一自治系统(Autonomous System)中进行决策路由。

目前,OSPF 已经成为广域网和企业网采用最多、应用最广泛的路由协议之一。目前用于 IPv4 的 OSPFv2 协议在 RFC 2328 中定义。为了让 OSPF 协议支持 IPv6,1999 年 IETF(国际互联网工程任务组)发布了 OSPFv3,它是由 RFC 5340 定义的。

7.1 OSPF 协议的工作原理

每台 OSPF 路由器通过 Hello 报文来发现邻居路由器,并建立邻接(Adjacency)。接着,每台路由器建立链路状态报文(Link-State Protocol Data Unit,LSP)。每台路由器将 LSP 泛洪到所有邻居。所有路由器会把收到的 LSP 存储在链路状态数据库(Link-State Data Base,LSDB)中。在网络中,同一区域的所有路由上的 LSDB 都达到一致。接着,每个路由器基于 LSDB 的信息,以自己为根结点,采用最短路径优先(Shortest Path First,SPF)算法计算到每个网络的最短路径,并将该路径保存到路由表中。

由于使用 SPF 算法计算路由,因此在算法上保证了没有路由环路。OSPF 通过邻居关系来维护路由,避免了定期更新对带宽的消耗。OSPF 路由更新效率高,网络收敛快。

OSPF 路由协议使用 SPF 算法计算路由的最佳路径。该算法是由一位荷兰的计算机科学家 Dijkstra 于 1959 年发明的,所以也称为 Dijkstra 算法。IS-IS 也使用 SPF 算法。

SPF 算法把网络考虑为一组点到点连接的结点,每条链路有一个成本(Cost)值,每个结点有它自己的名称及一个包含已知物理拓扑的完整链路信息的数据库。这里以图 7-1 所示的网络环境为例说明 SPF 算法。

图 7-1 描述了每台路由器到达邻居的成本,从路由器 A 出发到路由器 F,有两条链路,通过 SPF 算法将链路的成本值相加,结果为:

路由器 A→路由器 B→路由器 D→路由器 F 的成本值为 50。
路由器 A→路由器 C→路由器 E→路由器 F 的成本值为 97。

根据 SPF 算法的规定,路由器 A 到达路由器 F 的最佳路径为:

路由器 A→路由器 B→路由器 D→路由器 F

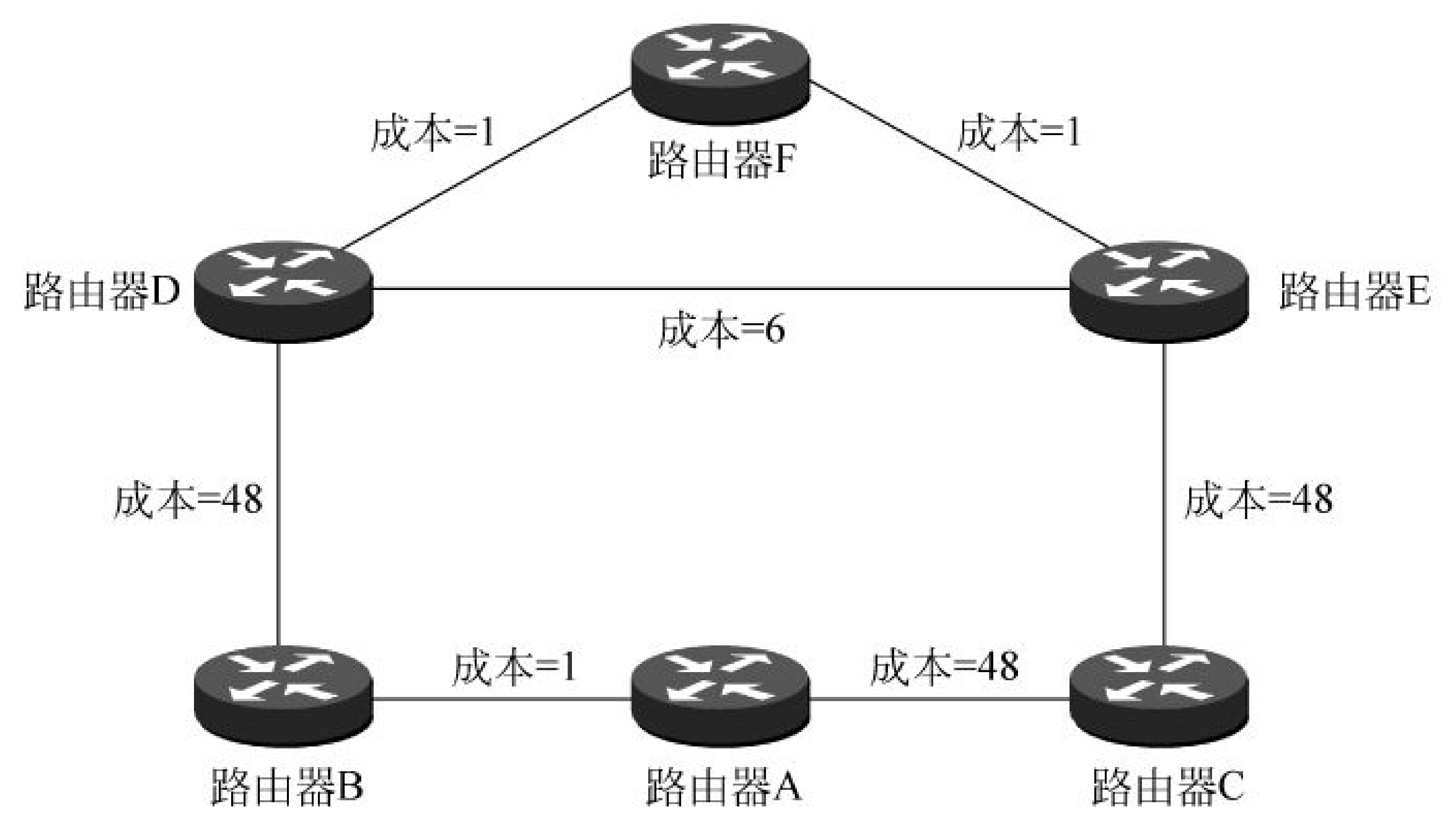


图 7-1　SPF 算法示例

从图 7-1 中可以看到，路由器 D 与路由器 E 之间还有一条链路，这对于网络本身来说造成了环路，无论这条链路的成本(Cost)值为多少，都不会列入 OSPF 路由协议的最佳路径中。OSPF 路由协议会使用 SPF 算法计算出一条路径优先树，以避免环路。

7.2　OSPF 报文

7.2.1　OSPF 报头格式

OSPF 使用了 Hello、数据库描述(DD)、链路状态请求(LSR)、链路状态更新(LSU)和链路状态确认(LSAck)5 种报文。这 5 种报文采用相同的报文头格式。其中，针对 IPv4 的 OSPFv2 协议报头大小为 24B。OSPFv2 协议的报头格式如图 7-2 所示。

0　　7	8　　15	16　　23	24　　31
Version	Type	Packet Length	
Router ID			
Area ID			
Checksum		AuType	
Authentication			

图 7-2　OSPFv2 协议的报头格式

每个字段的解析如下：

Version：版本字段，占 1 个字节，记录 OSPF 协议的版本号。

Type：报文类型字段，用于标识报文的类型，表示 OSPF 报文属于 5 种报文类型中的哪一种。

Packet Length：数据包长度字段，用于记录整个报文(包括报头部分和内容部分)的字节长度，长度单位为 Byte。该字段占 2 个字节。

Router ID：路由器 ID 字段，用于指定发送报文的源路由器 ID，占 4 个字节。

Area ID：区域 ID 字段，用于指定发送报文的路由器所在的 OSPF 区域号，占 4 个字节。

Checksum：报文的校验和字段，对整个报文的校验和，用于校验报文的正确性和完整性，占 2 个字节。

AuType：认证类型，指定认证类型，占 2 个字节。其中 0 表示不进行认证，1 表示进行简单认证，2 表示采用 MD5 方式进行认证。

Authentication：认证字段，占 4 个字节。当认证类型为 0 时，该字段无数据；当认证类型为简单认证时，该字段为认证密码；当认证类型为 MD5 时，该字段为 MD5 摘要消息。

针对 IPv6 的 OSPFv3 协议报头格式如图 7-3 所示。

0　　　7	8　　　15	16　　　23	24　　　31
Version	Type	Packet Length	
Router ID			
Area ID			
Checksum		Instance ID	0

图 7-3　针对 IPv6 的 OSPFv3 协议报头格式

其中，Version、Type、Packet Length、Router ID、Area ID 和 Checksum 字段与 OSPFv2 协议的字段意义相同。Instance ID 指的是 VPN(虚拟专用网络)的实例号，占 1 个字节。

7.2.2　OSPF 正文格式

以下是 OSPF 的 5 种报文正文的格式。

1. Hello 报文

OSPF 路由器使用组播地址 224.0.0.5 周期性地发送 Hello 报文，用于建立和维护相邻路由器之间的邻接关系。该报文用于向邻居路由器说明自己的存在，因此设计得比较简单，从而减少网络中的报文传输流量。Hello 报文被周期性(默认为 10s)地发送到邻居路由器接口。如果在 4 个周期内(即 40s 内)未收到 Hello 报文，则本地路由器会认为对方路由器已经失效。

OSPFv2 协议中的 Hello 报文格式如图 7-4 所示。每个字段的解析如下：

OSPFv2 Header：OSPF 头部，占 192 位。

Network Mask：发送 Hello 报文的接口所在的子网掩码。

Hello Interval：指定发送 Hello 报文的时间间隔，默认为 10s。

Options：可选项，取值 E 为允许泛洪 AS-external-LAS；取值 MC 为允许转发 IP 组播报文；取值 N/P 为允许处理 Type 7 LSA；取值 DC 为允许处理按需链路。

Rtr Pri：路由器优先级，默认值为 1。如果设置为 0，则表示该路由器不参加 DR/BDR 选举。

Router Dead Interval：指定路由器失效时间，默认为 40s。如果在此时间内未收到邻居发来的 Hello 报文，则认为邻居失效。

0　　7	8　　15	16　　23	24　　31
OSPFv2 Header(192位)			
Network Mask			
Hello Interval		Options	Rtr Pri
Router Dead Interval			
Designated Router			
Backup Designated Router			
Neighbor			
…			

图 7-4　OSPFv2 协议中的 Hello 报文格式

Designated Router：指定路由器的接口的 IP 地址。

Backup Designated Router：指定备份路由器的接口的 IP 地址。

Neighbor：邻居路由器的 ID。

下面的省略号(…)表示可以指定多个邻居路由器 ID。

OSPFv3 协议的 Hello 报文格式如图 7-5 所示。该格式和 OSPFv2 中的有细微差别。其中，Interface ID 是接口标识，在路由器上唯一标识接口。

0　　7	8　　15	16　　23	24　　31
OSPFv2 Header(128位)			
Interface ID			
Rtr Priority	Options		
Hello Interval		Router Dead Interval	
Designated Router			
Backup Designated Router			
Neighbor			
…			

图 7-5　OSPFv3 协议的 Hello 报文格式

2. 数据库描述报文

数据库描述(Database Description，DD)报文是用来描述本地路由器的链路状态数据库，用于两台相邻路由器进行链路状态数据库同步。当数据库的内容比较长的时候，需要多个 DD 报文来描述整个数据库。DD 报文交换过程按询问/应答方式进行。在 DD 报文交换

过程中，主路由器向从路由器发送它的路由表内容，并规定起始序列号，每发送一个 DD 报文，序列号加 1，从路由器则使用主路由器的序列号进行确定应答。OSPFv2 协议的 DD 报文格式如图 7-6 所示。每个字段的解析如下：

0　7	8　15	16　23	24　31
OSPFv2 Header(192位)			
Interface MTU		Options	00000 I M MS
DD Sequence Number			
LSA headers…			

图 7-6　OSPFv2 协议的 DD 报文格式

Interface MTU：接口最大传输单元，在不分段的情况下，此接口可发出的最大 IP 报文长度。

Options：可选项，取值 E 为允许泛洪 AS-external-LAS；取值 MC 为允许转发 IP 组播报文；取值 N/P 为允许处理 Type 7 LSA；取值 DC 为允许处理按需链路。

I(Initial)：初始化标志，发送连续多个 DD 报文时，如果这是第一个 DD 报文，则置为 1，否则置为 0。

M(More)：更多报文标志，连续发送多个 DD 报文时，如果这是最后一个 DD 报文，则置为 0，否则置为 1。

MS(Master/Slave)：设置进行 DD 报文双方的主从关系，如果本端是主路由器，则置为 1，否则置为 0。

DD Sequence Number：指定 DD 报文序列号。主从双方利用序列号来保证 DD 报文传输的可靠性和完整性。

LSA headers：指定 DD 报文中包括的 LSA 头部。后面的省略号(…)表示可以指定多个 LSA 头部。

OSPFv3 协议的 DD 报文格式和 OSPFv2 协议的 DD 报文格式相似，如图 7-7 所示。

0　7	8　15	16　23	24　31
OSPFv2 Header(128位)			
Interface MTU		Options	00000 I M MS
DD Sequence Number			
LSA headers…			

图 7-7　OSPFv3 协议的 DD 报文格式

3. 链路状态请求报文

当两台路由器之间相互交换 DD 报文后，如果发现邻居路由器的 LSDB 中有自己没有的或者已更新的链路状态信息时，该路由器会发送链路状态请求（Link State Request，

LSR)报文，向邻居路由器发出请求，从而获取相应的LSA(链路状态广播)。OSPFv2协议的LSR报文格式如图7-8所示。

0 7	8 15	16 23	24 31
OSPFv2 Header(192位)			
LS type			
Link State ID			
Advertising Router			
…			

图7-8 OSPFv2协议的LSR报文格式

LS type：指定所请求的LSA的类型。

Link State ID：链路状态标识，根据LSA的类型而定。

Advertising Router：指定产生此请求的LSA的路由器ID。

OSPFv3协议的LSR报文格式如图7-9所示。

0 7	8 15	16 23	24 31
OSPFv3 Header(128位)			
LS type			
Link State ID			
Advertising Router			
…			

图7-9 OSPFv3协议的LSR报文格式

4. 链路状态更新报文

当OSPF路由器接收到邻居路由器的LSR报文请求时，会通过链路状态更新(Link State Update，LSU)报文向对方发送相应的LSA，内容是多条LSA完整内容的集合。LSU报文在支持组播和广播的链路上以组播形式将LSA泛洪出去。OSPFv2协议的LSU报文格式如图7-10所示。

0 7	8 15	16 23	24 31
OSPFv2 Header(192位)			
Number of LSAs			
LSAs…			

图7-10 OSPFv2协议的LSU报文格式

Number of LSAs：指定此报文中共发送的 LSA 数量。

LSAs：是一条条具体的 LSA 完整信息，后面的省略号……表示可有多条 LSA。

OSPFv3 协议的 LSU 报文与 OSPFv2 协议的 LSU 报文类似。

5．链路状态确认报文

链路状态确认(Link State Acknowledgement，LSAck)报文用来对接收到的 LSU 报文进行确认。通过 LSAck 报文，可以增强 LSA 泛洪的可靠性。LSU 报文以组播方式将 LSA 泛洪出去，没有收到 LSAck 报文确认应答时，会对 LSA 进行重传，但重传时的 LSA 是直接送到没有收到确认应答的邻居路由器上，而不再是泛洪。报文仅包含 LSA Headers 字段，表示该报文包含的 LSA 头部。OSPFv2 协议的 LSAck 报文格式如图 7-11 所示。OSPFv3 协议的 LSAck 报文格式与 OSPFv2 协议的 LSAck 报文格式类似。

0　　7	8　　15	16　　23	24　　31
OSPFv2 Header(192位)			
LSAs Headers…			

图 7-11　OSPFv2 协议的 LSAck 报文格式

7.3　OSPF 分层结构

布局 OSPF 时，根据具体要求可以采用单域 OSPF 和多域 OSPF。一组运行 OSPF 路由协议的路由器，组成了 OSPF 路由器的自治域系统。同一个区域中的路由器是由同一个组织机构控制管理的，并且只运行一种 IGP 路由协议。路由器之间通常采用 BGP(边界网关协议)路由协议进行路由信息交换。单域 OSPF 指的是只有一个自治区域，如图 7-12 所示。当该区域要连接到互联网时，需要向相关组织申请自治域系统编号。当大量的路由器被分配到同一个自治区域时，会导致链路状态数据库(Link State Data Base，LSDB)十分庞大，占用大量的存储空间。此外，当存在大量的路由器时，网络拓扑结构发生变化的概率也大大增大。当网络拓扑变化时，需要传送大量的 OSPF 链路状态通告报文，大大降低了网络带宽的利用率。并且网络中的所有 OSPF 路由器都需要重新计算最优路径，耗费路由器的大量资源，降低路由器的运行效率。因此，单域 OSPF 结构不适用于大规模网络。

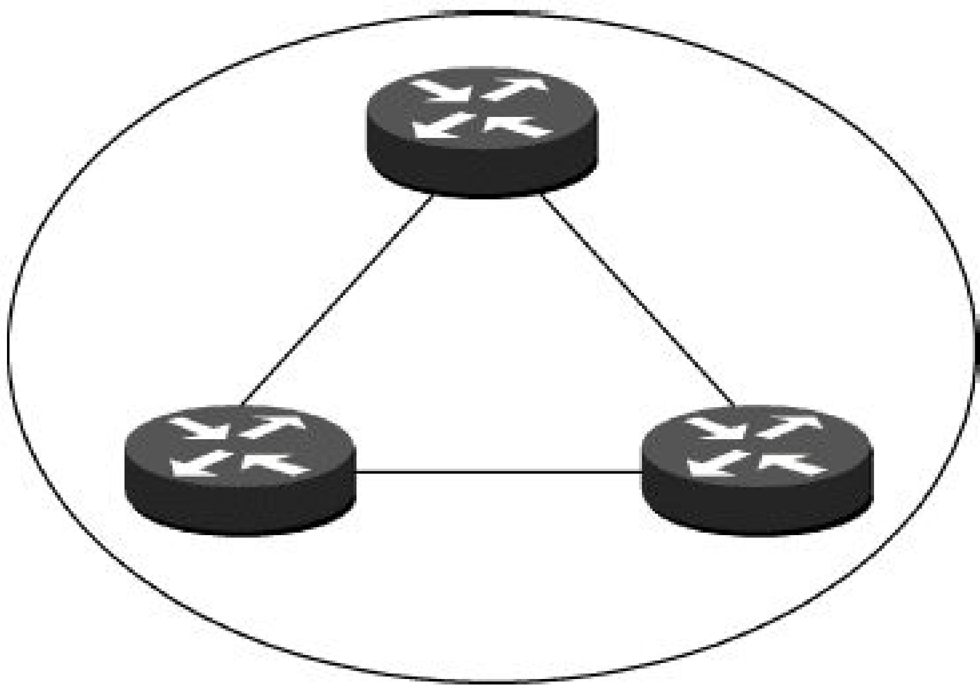


图 7-12　单域 OSPF

多域 OSPF 能够有效地解决以上问题。多域 OSPF 采用分层结构。OSPF 路由器被分隔成多个区域。每个区域都和一个主干区域进行直接连接。主干区域就像一道桥梁把所有区域连接起来，使其能够互相通信。如图 7-13 所示，区域 1 和区域 2 为非主干区域，它们通过主干区域进行连接。同一区域中的所有路由器都保持一个相同的链路状态数据库，每个路由器根据这一数据库建立自身的 SPF 树，建立路由表。不同区域中的路由器具有不同的链路状态数据库。当采用这种多区域的结构时，大部分的泛洪数据只会在自己的区域内进

行，只有少量的数据会传送到主干区域。这能够大大地减少泛洪时占用的网络资源。这种分层的方式也能够大大地减少链路状态数据库的大小，从而减少计算 SPF 路径时花费的运算资源。同时，这种分区的方式也能够提升安全性。

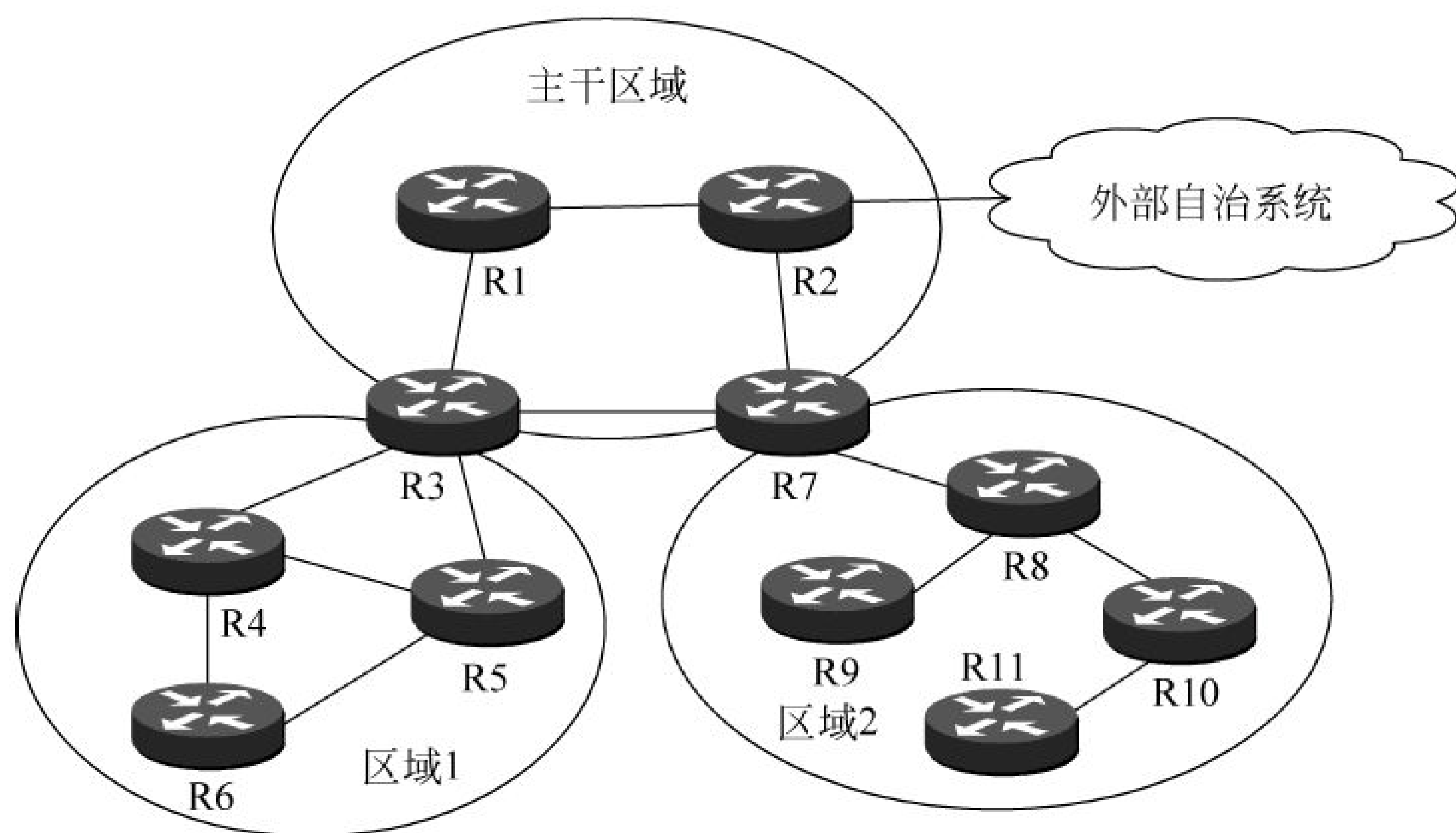


图 7-13　多域 OSPF

根据路由器所在的区域及作用，OSPF 路由器可分为内部路由器(Internal Router)、区域边界路由器(Area Border Router)、主干路由器(Backbone Router)和自治系统边界路由器(Autonomous System Boundary Router)。

1）内部路由器

内部路由器指的是所有接口都属于同一个 OSPF 区域，它们只保存区域内的链路状态信息。

2）区域边界路由器

该类型的路由器同时连接两个或两个以上的区域，其中一个区域必须为主干区域。区域边界路由器连接了主干区域和非主干区域，这种连接可以是物理上的连接，也可以是逻辑上的连接。

3）主干路由器

主干路由器指的是至少有一个接口位于主干区域的路由器。由此可见，区域边界路由器和位于主干区域里的路由器都属于内部路由器。

4）自治系统边界路由器

自治系统边界路由器指的是与其他自治系统交换路由信息的路由器。自治系统边界路由器可能是区域边界路由器，也可能是内部路由器。当一台 OSPF 路由器引入了外部路由的信息，它就是自治系统边界路由器。

根据图 7-13，R1、R4、R5、R6、R8、R9、R10 和 R11 都是内部路由器；R3 和 R7 为区域边界路由器；R1、R2、R3 和 R7 都是主干路由器；R2 为自治系统边界路由器。

7.4　OSPF 协议的工作过程

OSPF 协议的工作过程主要分为 5 个阶段：邻居发现、选举 DR/BDR、数据库同步、选择适当的路由器和维护路由信息。

1. 邻居发现

一台路由器加入 OSPF 区域时,首先会与邻居路由建立邻接关系,详细过程如图 7-14 所示。路由 1 向邻居路由 2 发送 Hello 报文并等待应答。这个报文是以组播的方式发送出去的,组播地址为 224.0.0.5。当路由 2 收到路由 1 发来的 Hello 报文时,会检查 Hello 中携带的参数,将收到来自路由 1 报文的接口转换为 Init 状态,同时路由 2 从接收到的 Hello 报文中获取路由 1 的 ID 并添加到邻居表中。接着,路由 2 会以组播的方式向所有直接连接的 OSPF 设备发送一个包含自己路由 ID 和路由 1 的 ID 的 Hello 报文。当路由 1 收到 Hello 报文后,发现里面具有自己的路由 ID,此时将收到来自路由 2 报文的接口状态转为 Two-way 状态。接着把路由 2 的 ID 添加到自己的邻居表中。

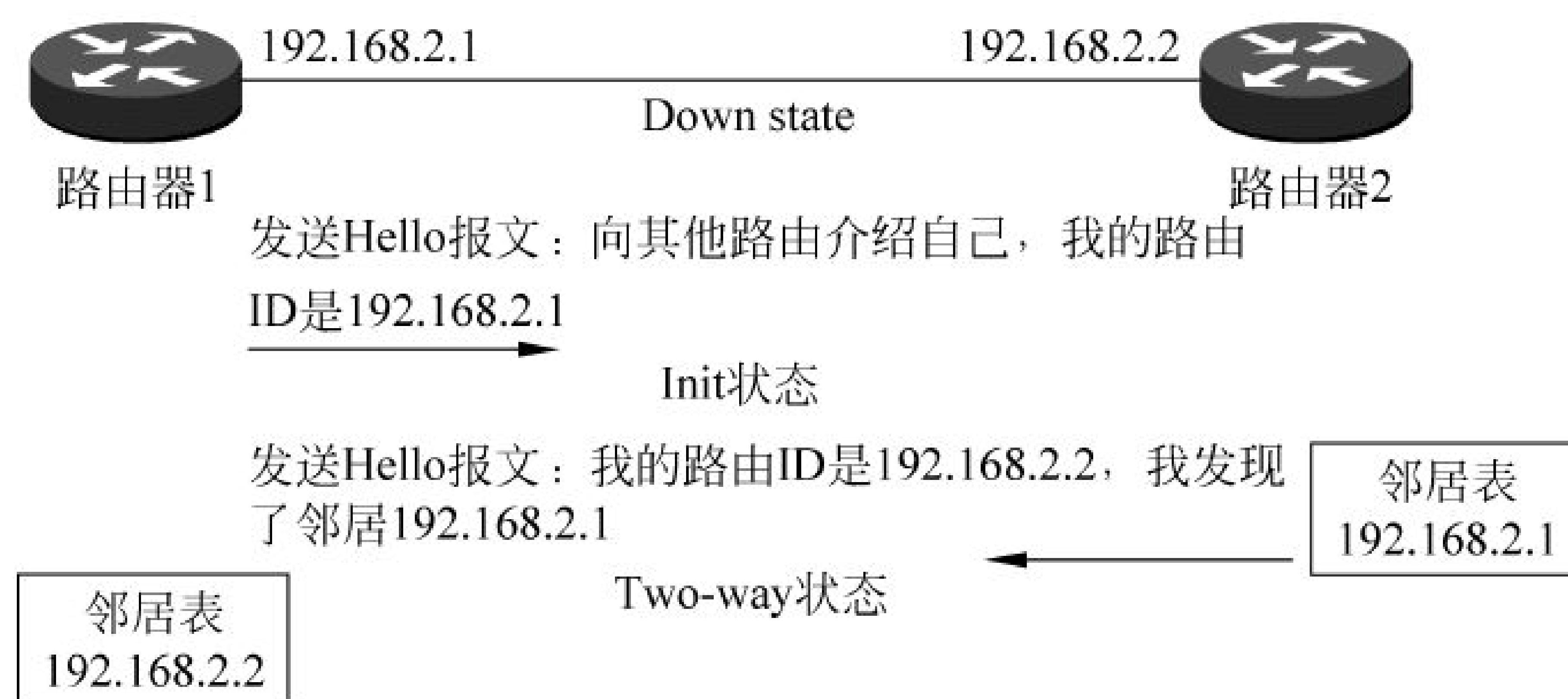


图 7-14　邻居发现过程

2. 选举 DR/BDR

如果在网络中任意两台路由器都建立邻接关系并交换路由信息,则需要建立 $n(n-1)/2$ 个邻接关系,其中 n 为路由器的数目。在网络上的路由器数量很多的情况下,如果每两台路由器之间都需要传递 LSA,就会导致大量的网络资源被占用。为了解决这一问题,在 OSPF 协议中会选定一台路由器作为指定路由器(Designated Router,DR),使其作为所有链路状态更新和 LSA 传递的集中点。所有路由器都会将路由信息发送给 DR,接着由 DR 将这些信息转发给本网段的其他路由器。也就是说,两台非 DR 的路由器之间不再需要交换路由信息。该方式大大降低了传递 LSA 占用的网络资源。此外,OSPF 协议还设置了备份指定路由器(Backup Designated Router,BDR)。当 DR 失效时,BDR 会立即成为 DR。因此,BDR 也会与其他路由器建立邻接关系。由于不需要重新选举,并且 BDR 和其他路由器的邻接关系已经建立,所以这个接替过程十分短暂。此时还需要重新选举出一个新的 BDR。这需要较长的时间,但并不会影响路由计算。

当与邻居建立双向通信之后,路由器会检查邻居的 Hello 包中的优先级(Priority)字段、DR 和 BDR 字段,并声明自己就是 DR/BDR,其中 Hello 包中 DR 和 BDR 字段的值就是它们自己的接口地址。优先级高的路由器将会胜出,成为 DR。如果优先级相等,则路由 ID 较大者将会被选举为 DR。选举 DR/BDR 的过程如图 7-15 所示。

3. 数据库同步

此时路由器相互交换链路状态信息。每个路由器对收到的信息进行分析,当发现收到的链路状态信息不在当前的链路状态数据库时,路由器会发送链路状态请求(LSR),要求对



图 7-15 选举 DR/BDR 的过程

方传送完整的链路状态信息。此时，对方会发送链路状态更新(LSU)报文回送所需要的信息。这个状态完成后，路由器之间建立完全邻接(Full Adjacency)关系。此时实现了相邻路由器之间的链路状态数据库同步，同步过程如图 7-16 所示。

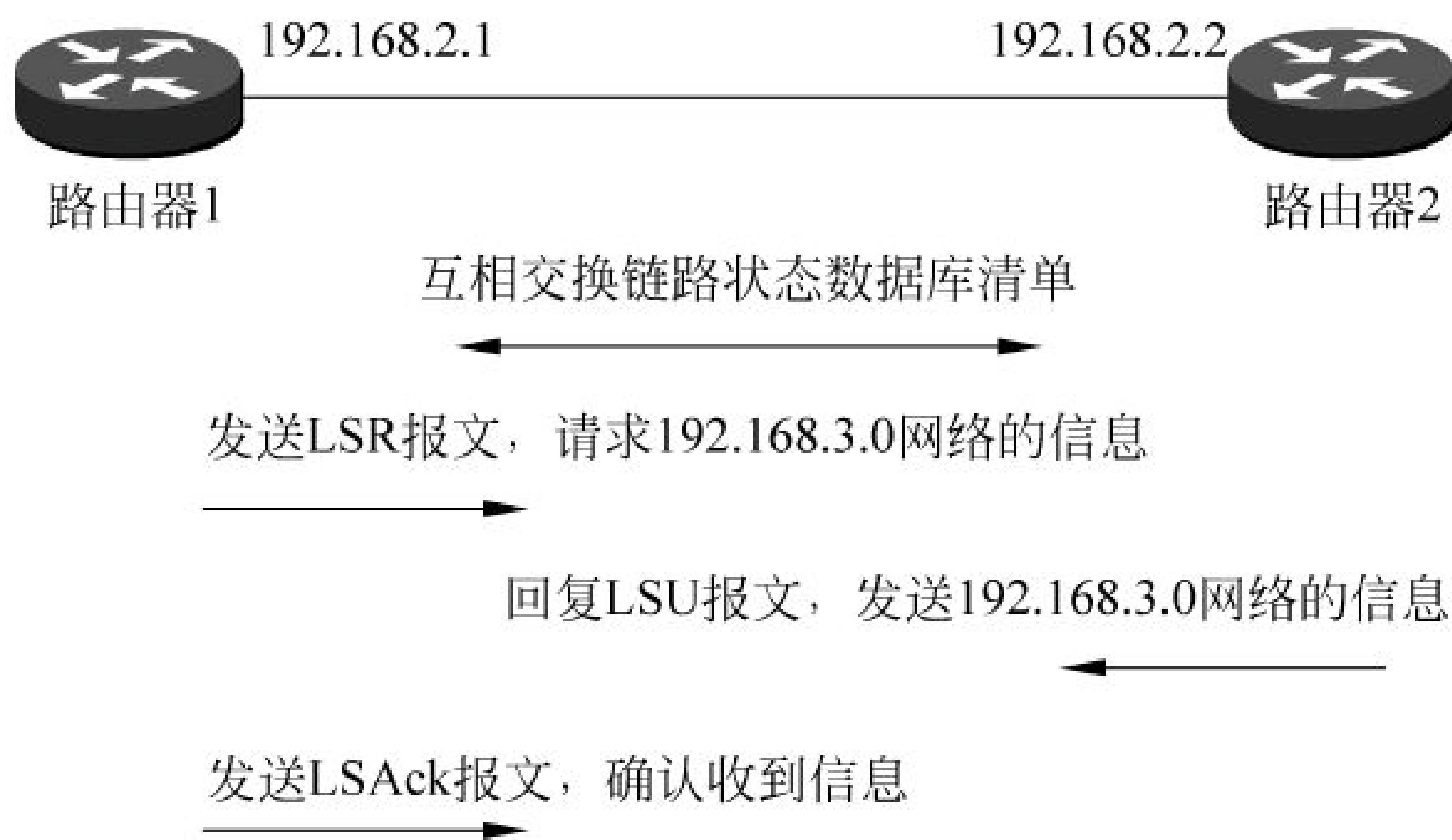


图 7-16 数据库同步过程

4. 选择适当的路由器

当路由器具有完整的链路状态数据库时，每个路由器根据链路状态数据库的内容，通过使用 SPF 算法计算出到目的网络的最短路径，并把它们添加到自己的路由表中。OSPF 协议采用成本来表示路径的长度。通常可以根据链路的时延、带宽等来设置链路的成本。

5. 维护路由信息

当网络中链路状态发生变化时，OSPF 会生成 LSA，并以泛洪的方式通知网络上的其他路由器。当路由器收到 LSA 更新报文时，如果该 LSA 不存在于 LSDB 中，路由器就会发送 LSAck 报文进行确认，接着会将该 LSA 泛洪出去。当收到的 LSA 已经存在于 LSDB 中时，路由器会检查该 LSA 序列号和 LSDB 中的是否相同。如果相同，则忽略该 LSA。如果该 LSA 的序列号大于 LSDB 中的序列号，则证明收到的是更新后的 LSA。此时需要把它添加到 LSDB 中，并发送 LSAck 报文进行确认。最后把该 LSA 泛洪出去。当收到的 LSA 的序列号小于 LSDB 中的序列号时，证明该 LSA 是旧的 LSA，这可能是由于网络拥塞等原因造成。此时，路由器将会忽略该 LSA。当更新完 LSDB 后，路由器会使用 SPF 算法重新计算路由表。重新计算路由表需要一定的时间。

7.5 OSPF 配置与管理

7.5.1 OSPFv2 配置与管理

无论哪种路由器,都必须支持 OSPF 协议。通常,路由器的 OSPF 协议参数都会有默认设置。例如,OSPF 报文的发送间隔,计算 SPF 路径的时间间隔等。当然,这些参数也可以通过命令进行设置。以下是配置 OSPF 协议的基本过程。

1. 启动 OSPF 进程

启动 OSPF 进程的命令如下:

```
Router(config)#router ospf id
```

其中,id 是进程号,由网络管理员指定,其范围为 1~65 535。该命令的作用是启动 OSPF 路由,并进入配置模式。一台路由器可以启动一个或多个 OSPF 进程。

接着定义 OSPF 运行的接口和该接口的区域号:

```
Router(config-router)#network ip-address wildcard-mask area area-id
```

ip-address 是接口的地址; wildcard-mask 为通配符掩码; area-id 是区域号,其中 0 表示主干区域,在配置 OSPF 时,必须指定它所属于的区域号。

2. 配置 OSPF 接口参数

通过 interface 命令能够配置接口类型,并进入接口配置模式:

```
Router(config)#interface type-number
```

在 OSPF 协议中,需要计算每个路由器到目标网络的最短路由,这就要求我们定义每条路径的成本(即 Cost)。数据包到达目的网络,途经的每条链路的 Cost 指的是发送时加上该发送接口的 Cost,而接收时不需要加上接口的 Cost。在 Cisco 中,Cost 的度量值为 100MB/带宽。

在 OSPF 路由的设置中,可以采用以下命令定义在一个 OSPF 接口上发送一个数据包需要花费的成本:

```
Router(config-if)# ip ospf cost cost-value
```

然而,目前的网络带宽比较大,如果以 100MB 作为参考值,会使大部分链路的 Cost 都为 1(Cost 只能用整数表示),这样不利于选路。因此,建议使用时把网络带宽参考值设得大一点,如设为 10GB:

```
Router(config-router)# auto-cost reference-bandwith 10000
```

对于每个 OSPF 路由器,它们都有自己的优先级。该优先级主要用于决定哪个路由器将会成为 DR 和 BDR。通过以下命令设置 OSPF 路由器的优先级:

```
Router(config-if)# ip ospf priority number-value
```

该命令中,number-value 指的是路由器的优先级,范围为 0~255,默认值为 1,值越大,优先级越高。当 number-value 为 0 时,表示该路由器不会被选举为 DR/BDR。对于路由器

的每个接口，都可以设置一个不同的优先级。

3. 查看配置好的路由信息

以下是查看路由相关信息的常用命令：

```
show ip route                         //查看路由表信息
show ip ospf interface                //查看区域号和相关的信息
show ip ospf neighbor                 //查看接口上的邻居信息
show ip ospf database                 //查看链路状态数据库
```

下面以图 7-17 所示的网络环境为例，说明 OSPF 的配置和管理命令。

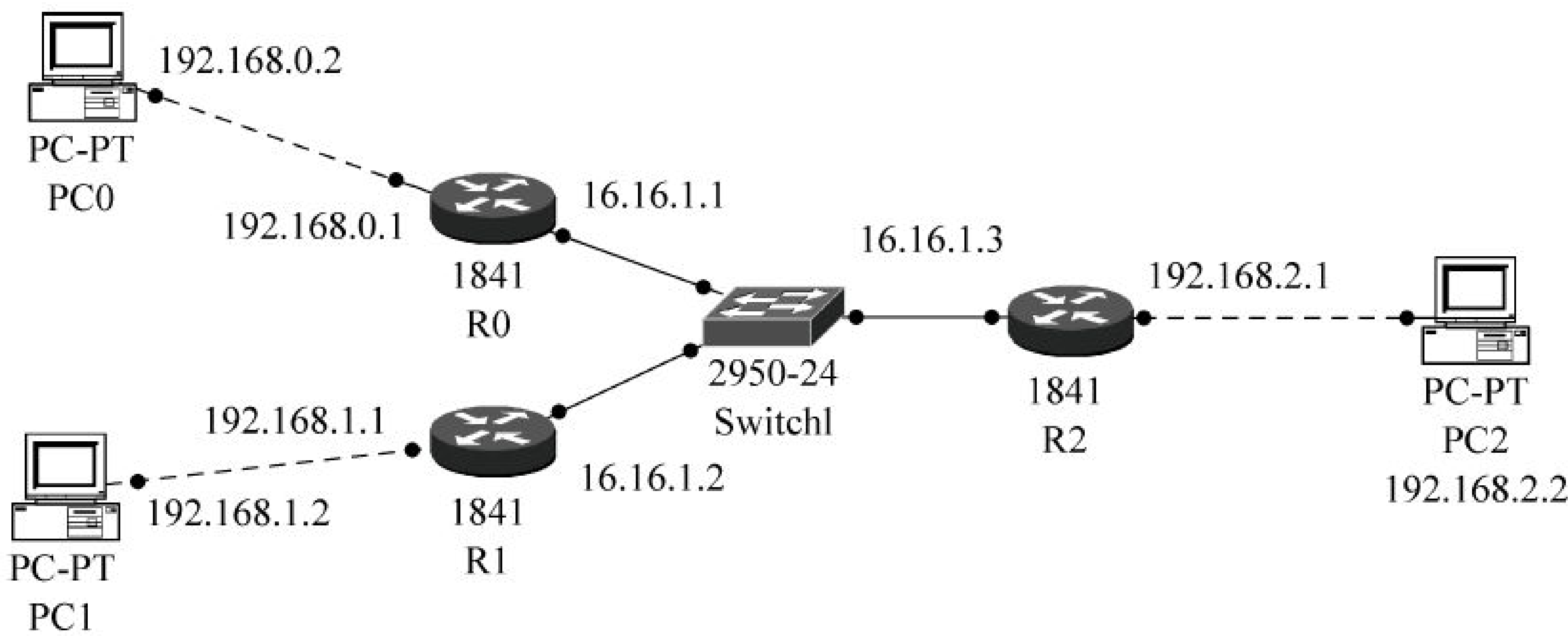


图 7-17 OSPFv2 的配置环境

分别在每个路由器上配置、启动 OSPF 路由，并且通告网络及所在的区域，具体命令如图 7-18 所示。

```
Router0(config)#router ospf 1
Router0(config-router)#router-id 192.168.0.1
Router0(config-router)#network 192.168.0.0 255.255.255.0 area 0
Router0(config-router)#network 16.16.1.0 255.255.255.0 area 0
Router0(config-router)#auto-cost reference-bandwidth 1000

Router1(config)#router ospf 1
Router1(config-router)#router-id 192.168.1.1
Router1(config-router)#network 192.168.1.0 255.255.255.0 area 0
Router1(config-router)#network 16.16.1.0 255.255.255.0 area 0
Router1(config-router)#auto-cost reference-bandwidth 1000

Router2(config)#router ospf 1
Router2(config-router)#router-id 192.168.2.1
Router2(config-router)#network 192.168.2.0 255.255.255.0 area 0
Router2(config-router)#network 16.16.1.0 255.255.255.0 area 0
Router2(config-router)#auto-cost reference-bandwidth 1000
```

图 7-18 配置路由器

配置完成后，可以使用路由器 R1 作为参考点，分别通过命令 show ip route、show ip ospf neighbor、show ip ospf interface 进行验证。

首先通过命令 show ip route 来查看路由表信息，结果如图 7-19 所示。从图 7-19 中可看出，R1 成功地学习到了路由器 R0 和 R2 公告出来的 OSPF 路由，其中的 O 就表示通过 OSPFv2 所学到的路由。

通过命令 show ip ospf neighbor 查看接口上的邻居信息，结果如图 7-20 所示。Neighbor ID 指的是邻接路由器的路由 ID。在本例中，是通过 router-id x. x. x. x 手工配置的。Pri 指

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     16.0.0.0/24 is subnetted, 1 subnets
C       16.16.1.0 is directly connected, FastEthernet0/1
O    192.168.0.0/24 [110/2] via 16.16.1.1, 00:36:36, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/2] via 16.16.1.3, 00:36:36, FastEthernet0/1

Router1#
```

图 7-19　查看路由表信息

的是邻接路由器的优先级。State 字段表示邻接路由器的功能状态。FULL 意味着路由器与邻居是完全相邻关系，DR 意味着它是指定路由器。由此可知，路由器 R0 是 DR 路由器。Dead Time 指的是失效时间，表示路由器在声明邻居断开之前等待从邻居接收 OSPF Hello 数据包的剩余时间。示例中，如果在 32s 内路由器没有接收到邻居 192.168.2.1 的 Hello 数据包，则声明邻居断开。Address 字段表示此相邻是直接连接接口的 IP 地址。Interface 表示与 OSPF 邻居形成了邻接关系的接口。

```
Router1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.0.1       1   FULL/DROTHER    00:00:32    16.16.1.1       FastEthernet0/1
192.168.2.1       1   FULL/DR         00:00:32    16.16.1.3       FastEthernet0/1
```

图 7-20　查看接口上的邻居信息

通过命令 show ip ospf interface 查看区域号和相关的信息，结果如图 7-21 所示。该命令列出了 Internet Address、Area、Process ID、Router ID、Network Type、Cost、Transmit Delay、State、Priority、Designated Router、Backup Designated Router、Timer intervals、Neighbor Count、Adjacent with neighbor 等信息。从这些信息中可以看出，本路由器是 BDR。路由器有两个邻居，其中路由 ID 为 192.168.2.1 的路由器为 DR，因为它的 IP 地址比较大。

图 7-22 通过 show ip ospf database 命令来查看路由器 R1 的链路状态数据库。第 2 行显示了路由器的 ID 号和 OSPF 进程号。接下来显示的是区域 0 中的路由器链路状态信息。Link ID 指的是 Link-State ID，它代表整个路由器，而不是代表某个链路。ADV Router 指的是通告链路状态信息的路由器的 ID 号，即 Link ID 名下的内容是由它通告的。Age 指的是 LSA 条目的老化时间(1 800 s 到期)。Seq # 指的是 LSA 的序列码。Checksum 描述的是 LSA 的校验和。Link count 指的是通告路由器(ADV Router)在本区域的链路数目。接下来描述的是区域 0 中的网络链路状态信息。

```
Router1#show ip ospf interface

FastEthernet0/1 is up, line protocol is up
 Internet address is 16.16.1.2/24, Area 0
 Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 1
 Designated Router (ID) 192.168.2.1, Interface address 16.16.1.3
 Backup Designated Router (ID) 192.168.1.1, Interface address 16.16.1.2
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:07
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.0.1
  Adjacent with neighbor 192.168.2.1  (Designated Router)
 Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:07
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
```

图 7-21　查看区域号和相关的信息

```
Router1#show ip ospf database
            OSPF Router with ID (192.168.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.1.1     192.168.1.1     94          0x80000007 0x00d0e4 2
192.168.2.1     192.168.2.1     103         0x80000006 0x003280 2
192.168.0.1     192.168.0.1     103         0x80000006 0x0010aa 2

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
16.16.1.3       192.168.2.1     98          0x80000004 0x0089b6
Router1#
```

图 7-22　查看链路状态数据库

7.5.2　OSPFv3 配置与管理

OSPFv3 主要用于 IPv6 网络，它是在 OSPFv2 基础上开发的适用于 IPv6 网络的路由协议。OSPFv3 具有 OSPFv2 相似的工作机制。然而，为了支持 IPv6 地址格式，OSPFv3 对 OSPFv2 做了一些改进。和 OSPFv2 一样，OSPFv3 在工作过程中也需要进行组播。在 OSPFv2 中，DR 路由器组播时使用 224.0.0.6 地址，其他路由器组播时使用 224.0.0.5 地址。而在 OSPFv3 中，DR 路由器组播时采用 FF02::6 地址，其他路由器采用 FF02::5 地址进行组播。

在数据包类型、区域划分、路由器类型、邻居发现、邻接关系形成方式、LSA 泛洪、DR 选举机制和路由计算方法上，OSPFv2 和 OSPFv3 是一样的。在 OSPFv2 中，只有在同一个子

网中的路由器才能形成邻居关系。然而,OSPFv3 是基于链路运行的,一个链路可以划分为多个 IPv6 前缀(类似于子网的概念),结点即使不在同一个前缀范围,只要在同一链路上,也可以形成邻居关系。

在 OSPFv2 中,路由 ID 是一个可选项。当 OSPF 运行在广播网络时,通过路由器的接口地址标识,然而其他链路的 OSPFv2 的邻居则是通过路由器 ID 来标识。OSPFv3 对这个不一致性进行了改进,对所有的链路全部使用路由 ID 来识别邻居。因此,OSPFv3 的路由 ID 项是必须进行设置的,否则无法启动。

以下是 OSPFv3 常用的配置命令。

1)设置路由器 ID

当没有任何接口配置 IPv4 地址时,则必须使用如下命令为路由器设置 ID 号:

```
Router(config)# ipv6 router ospf id
```

其中,id 是进程号。

2)启用 OSPF

通过以下命令在接口上启用 OSPF,把接口置于某个 OSPF 进程的某个区域中,同时还可以声明其使用的实例编号。

```
Router(config)# ipv6 ospf process - id area area - id [instance instance - id]
```

其中,process-id、area-id 和 instance-id 分别为进程号、区域号和实例号。

下面以图 7-23 所示的网络环境为例,说明 OSPF 的配置和管理命令。分别在路由器 R0、R1、R2 上配置 3 个环回接口,分别配置 3 个单播范围内的 IPv6 地址,模拟 3 个不同的 IPv6 前缀,然后在 3 台路由器上启动 OSPFv3。

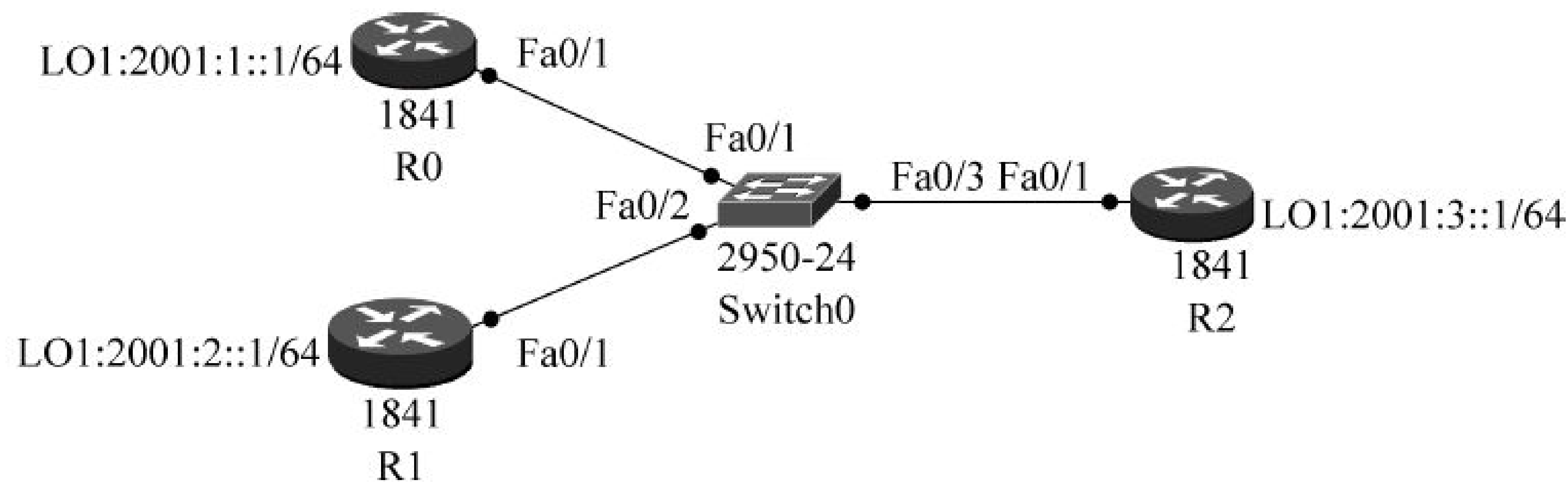


图 7-23 OSPFv3 的配置环境

在路由器 R0、R1 和 R2 上配置、启动 OSPF 路由,并且通告网络及所在的区域,具体配置如图 7-24 所示。

配置完成后,可以通过命令 show ipv6 route 查看路由器 R1 的 IPv6 路由表,如图 7-25 所示,可以看出 R1 成功地学习到了路由器 R0 和 R2 公告出来的 OSPF 路由,其中的 O 表示通过 OSPFv3 学到的路由。

通过命令 show ipv6 ospf neighbor 查看 OSPFv3 的邻居关系正常,如图 7-26 所示。从图 7-26 中可以看出 R1 路由器有两个邻居,并且可知路由器 R0 是 DR 路由器。

```
Router0(config)#ipv6 router ospf 1
Router0(config-rtr)#router-id 1.1.1.1
Router0(config-rtr)#exit
Router0(config)#interface Fa0/1
Router0(config-if)#ipv6 ospf 1 area 0
Router0(config-if)#exit
Router0(config)#interface loopback1
Router0(config-if)#ipv6 ospf 1 area 0

Router1(config)#ipv6 router ospf 1
Router1 (config-rtr)#router-id 2.2.2.2
Router1 (config-rtr)#exit
Router1 (config)#interface Fa0/1
Router1 (config-if)#ipv6 ospf 1 area 0
Router1 (config-if)#exit
Router1 (config)#interface loopback1
Router1 (config-if)#ipv6 ospf 1 area 0


Router2(config)#ipv6 router ospf 1
Router2 (config-rtr)#router-id 3.3.3.3
Router2 (config-rtr)#exit
Router2 (config)#interface Fa0/1
Router2 (config-if)#ipv6 ospf 1 area 0
Router2 (config-if)#exit
Router2 (config)#interface loopback1
Router2 (config-if)#ipv6 ospf 1 area 0
```

图 7-24 配置 OSPFv3 路由器

```
R1#show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O      2001:1::1/128 [110/1]
            via FE80::201:C9FF:FEB1:3C02, FastEthernet0/1
C      2001:2::/64 [0/0] via ::, Loopback1
L      2001:2::1/128 [0/0] via ::, Loopback1
O      2001:3::1/128 [110/1] via FE80::20A:41FF:FEDC:9DAA, FastEthernet0/1
L      FF00::/8 [0/0] via ::, Null0
```

图 7-25 查看路由表

```
R1#show ipv6 ospf neighbor
Neighbor ID Pri     State              Dead Time     Interface ID     Interface
1.1.1.1       1     FULL/DR        00:00:38          2               FastEthernet0/1
3.3.3.3       1     FULL/DROTHER   00:00:36          2               FastEthernet0/1
```

图 7-26 查看邻居表

7.6 本章总结

开放最短路径优先(Open Shortest Path First,OSPF)协议是一种内部网关协议(Interior Gateway Protocol,IGP)。

每个路由器基于LSDB(链路状态数据库)的信息,以自己为根结点,采用最短路径优先(Shortest Path First,SPF)算法计算到每个网络的最短路径,并将该路径保存到路由表中。

OSPF使用了Hello、DD、LSR、LSU和LSAck 5种报文。

OSPF路由器使用组播地址224.0.0.5周期性地发送Hello报文,用以建立和维护相邻路由器之间的邻接关系。

数据库描述(Database Description,DD)报文是用来描述本地路由器的链路状态数据库,用于两台相邻路由器进行链路状态数据库同步。

当两台路由器之间相互交换DD报文后,如果发现邻居路由器的LSDB中有自己没有的或者已更新的链路状态信息时,该路由器会发送链路状态请求(Link State Request,LSR)报文,向邻居路由器发出请求,从而获取相应的LSA。

链路状态确认(Link State Acknowledgement,LSAck)报文用来对接收到的LSU报文进行确认。通过LSAck报文,可以增强LSA泛洪的可靠性。

布局OSPF时,根据具体要求可以采用单域OSPF和多域OSPF。一组运行OSPF路由协议的路由器,组成了OSPF路由器的自治域系统。

当大量的路由器被分配到同一个自治区域时,会导致链路状态数据库(Link State Data Base,LSDB)十分庞大,占用大量的存储空间。此外,当存在大量的路由器时,网络拓扑结构发生变化的概率也大大增大。因此,单域OSPF结构不适用于大规模网络。

多域OSPF能够有效地解决以上问题。多域OSPF采用分层结构。OSPF路由器被分隔成多个区域。每个区域都和一个主干区域进行直接连接。主干区域就像一道桥梁,把所有区域连接起来,使其能够互相通信。

根据路由器所在的区域及作用,OSPF路由器可分为内部路由器(Internal Router)、区域边界路由器(Area Border Router)、主干路由器(Backbone Router)和自治系统边界路由器(Autonomous System Boundary Router)。

OSPF协议的工作过程主要分为5个阶段:邻居发现、选举DR/BDR、数据库同步、选择适当的路由器和维护路由信息。

在OSPF协议中会选定一台路由器作为指定路由器(Designated Router,DR),使其作为所有链路状态更新和LSA传递的集中点。所有路由器都会将路由信息发送给DR,接着由DR将这些信息转发给本网段的其他路由器。也就是说,两台非DR的路由器之间不再需要交换路由信息。该方式大大降低了传递LSA占用的网络资源。此外,OSPF协议还设置了备份指定路由器(Backup Designated Router,BDR)。当DR失效时,BDR会立即成为DR。

启动OSPF进程的命令如下:

```
Router(config)#router ospf id
```

其中 id 是进程号，由网络管理员指定，其范围为 1～65 535。该命令的作用是启动 OSPF 路由，并进入配置模式。一台路由器可以启动一个或多个 OSPF 进程。

接着定义 OSPF 运行的接口和该接口的区域号：

```
Router(config-router)# network ip-address wildcard-mask area area-id
```

ip-address 是接口的地址；wildcard-mask 为通配符掩码；area-id 是区域号，其中 0 表示主干区域，配置 OSPF 时，必须指定它所属的区域号。

对于每个 OSPF 路由器，它们都有自己的优先级。该优先级主要用于决定哪个路由器将会成为 DR 和 BDR。通过以下命令设置 OSPF 路由器的优先级。

```
Router(config-if)# ip ospf priority number-value
```

该命令中的 number-value 指的是路由器的优先级，范围为 0～255，默认值为 1，该值越大，优先级越高。当 number-value 设置为 0 时，表示该路由器不会被选举为 DR 和 BDR。

以下是查看路由相关信息的常用命令：

```
show ip route                        //查看路由表信息
show ip ospf interface               //查看区域号和相关的信息
show ip ospf neighbor                //查看接口上的邻居信息
show ip ospf database                //查看链路状态数据库
```

为了支持 IPv6 地址格式，OSPFv3 对 OSPFv2 做了一些改进。和 OSPFv2 一样，OSPFv3 在工作过程中也需要进行组播。在 OSPFv2 中，DR 路由器组播时使用 224.0.0.6，其他路由器组播时使用 224.0.0.5。而在 OSPFv3 中，DR 路由器组播时采用 FF02::6 地址，其他路由器采用 FF02::5 地址进行组播。

在数据包类型、区域划分、路由器类型、邻居发现、邻接关系形成方式、LSA 泛洪、DR 选举机制和路由计算方法上，OSPFv2 和 OSPFv3 是一样的。在 OSPFv2 中，只有在同一个子网中的路由器，才能形成邻居关系。然而，OSPFv3 是基于链路运行的，一个链路可以划分为多个 IPv6 前缀(类似于子网的概念)，结点即使不在同一个前缀范围，只要在同一链路上，也可以形成邻居关系。

OSPFv3 常用的配置命令。

(1) 设置路由器 ID。

当没有任何接口配置了 IPv4 地址时，则必须使用如下命令为路由器设置 ID 号：

```
Router(config)# ipv6 router ospf id
```

其中 id 是进程号。

(2) 启用 OSPF。

通过以下命令在接口上启用 OSPF，把接口置于某个 OSPF 进程的某个区域中，同时还可以声明其使用的实例编号。

```
Router(config)# ipv6 ospf process-id area area-id [instance instance-id]
```

其中，process-id、area-id 和 instance-id 分别为进程号、区域号和实例号。

复习思考题

1. OSPF 协议的工作原理是什么?
2. 请分别画图说明 OSPFv2 和 OSPFv3 协议的报头格式。
3. OSPF 协议包括哪几种报文?请分别画图说明每种报文的格式。
4. 为什么单域 OSPF 结构不适用于大规模网络?
5. 在多域 OSPF 结构中,路由器分为哪几种类型?
6. 什么是 DR?什么是 BDR?OSPF 是怎样选举 DR 和 BDR 的?
7. OSPFv2 的配置和管理使用哪些命令?请逐一说明每个命令的格式和功能。
8. OSPFv3 的配置和管理使用哪些命令?请逐一说明每个命令的格式和功能。
9. 实训操作题 1:请参照图 7-27 所示的网络环境为每个路由器配置 OSPFv2 协议。

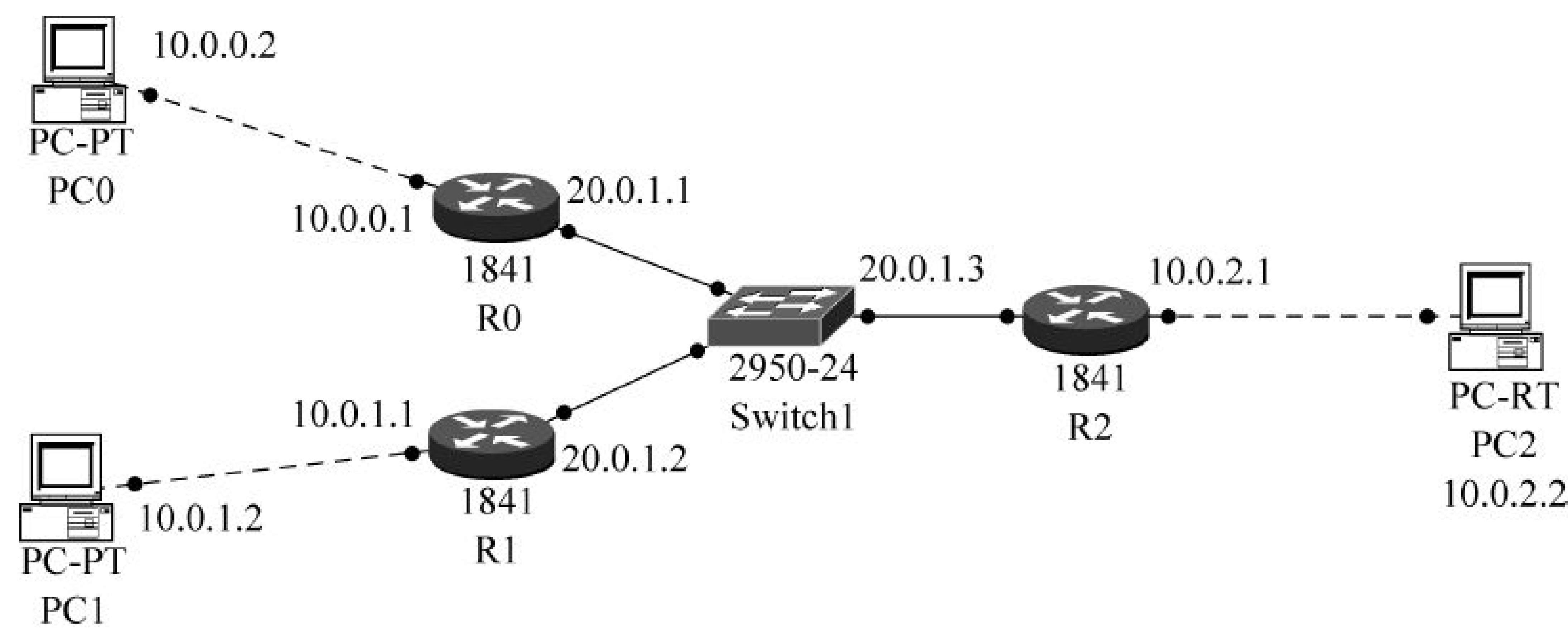


图 7-27 实训操作题 1 的 OSPFv2 协议配置环境

10. 实训操作题 2:请参照图 7-28 所示的网络环境为每个路由器配置 OSPFv3 协议。

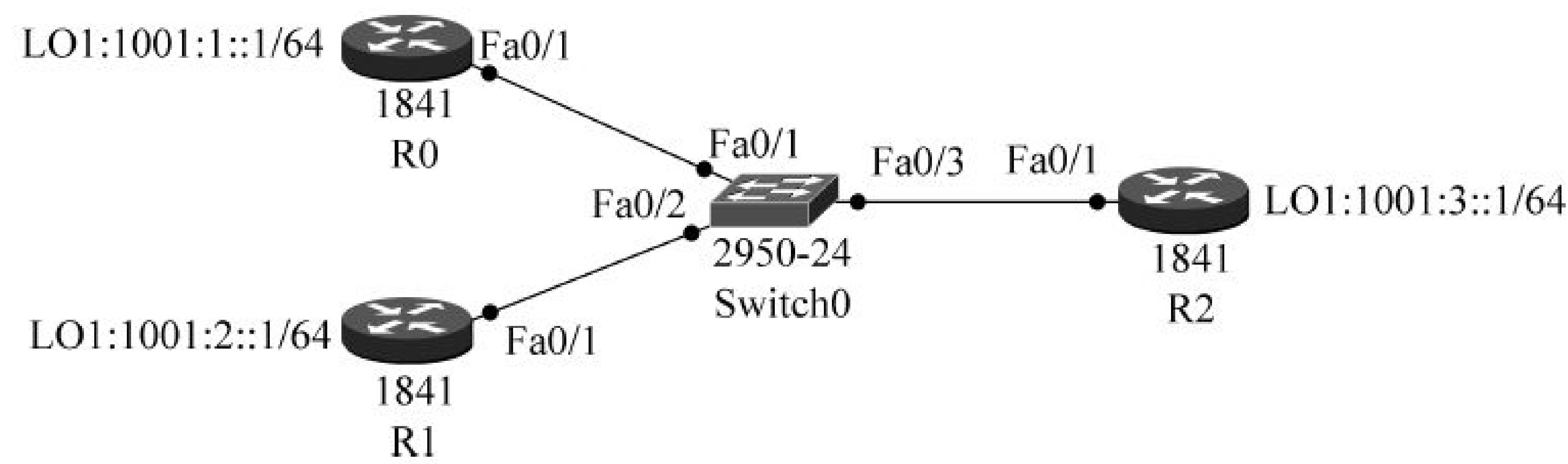


图 7-28 实训操作题 2 的 OSPFv3 协议配置环境

第8章 EIGRP

CHAPTER 8

增强型内部网关路由协议(Enhanced Interior Gateway Routing Protocol,EIGRP)原来是Cisco公司的私有协议。Cisco公司直到2013年3月才将EIGRP路由协议以RFC文档的形式呈交给国际互联网工程任务组(The Internet Engineering Task Force,IETF),使EIGRP协议公有化。EIGRP协议综合了链路状态和距离矢量型路由选择协议这两种技术,采用扩散更新算法(Diffusing Update ALgorithm,DUAL)来实现快速收敛,可以不发送定期的路由更新信息,以减少带宽的占用,并能够支持Apple Talk、IP、Novell和NetWare等多种网络层协议。

8.1 EIGRP概述

8.1.1 IGRP与EIGRP

增强型内部网关路由协议的前身是内部网关路由协议(Interior Gateway Routing Protocol,IGRP)。IGRP也是Cisco的私有协议,是基于距离向量的路由协议。虽然IGRP同样适用于规模较小的局域网,但是,与RIP路由协议有所不同,IGRP使用TCP层的端口号9来进行报文交换,而RIP则使用TCP层的端口号520进行报文交换。

IGRP是由Cisco公司于20世纪80年代中期设计并推出的,同时使用延迟、带宽、可靠性和负载等因素来确定最佳路由。默认状态下,IGRP以90s为周期,每个周期发送一次路由更新信息,在3个更新周期(即270s)内如果没有接收到某个路由器发送的更新信息,则会宣布该路由器不可访问。在第7个更新周期(即630s)之后,IGRP会从路由表中清除该路由。

增强型内部网关路由协议是综合了链路状态算法和距离矢量型路由选择算法的Cisco专用协议。自从EIGRP路由协议诞生后,IGRP路由协议就逐渐被淘汰了。

EIGRP是由距离矢量算法和链路状态算法混合而成的。因此,EIGRP既可以像距离矢量协议那样从它的相邻路由器那里得到更新信息,也可以像链路状态协议那样,保存着一个拓扑表,并且通过自己的DUAL选择一个最佳的无环路径。

不同于传统的距离矢量协议,EIGRP有很短的收敛时间,而且不用定期发送路由更新信息;也不像RIP,并不知道整个网络的状态,只能靠邻居公布的信息。EIGRP使用与IGRP相同的路由算法,即DUAL。DUAL是EIGRP的核心,通过它来实现无环路由。内部EIGRP管理距离为90,外部EIGRP管理距离为170,支持等价和非等价负载均衡。IP数据包中,EIGRP的协议字段取值为88。

8.1.2 EIGRP 的优点

EIGRP 是 Cisco 的私有路由协议，它综合了距离矢量算法和链路状态算法这两种技术，它的优点主要包括以下 7 个方面。

1. 快速收敛

EIGRP 采用 DUAL 来实现快速收敛。运行 EIGRP 的路由器存储了邻居的路由表，因此能够快速适应网络中的变化。如果本地路由表中没用合适的路由且拓扑表中没用合适的备用路由，EIGRP 将查询邻居，以发现替代路由。查询将不断执行，直到找到替代路由或确定不存在替代路由。

2. 部分更新

EIGRP 发送部分更新，而不是定期更新，且仅在路由路径或者度量值发生变化时才发送。更新中只包含已变化的链路的信息，而不是整个路由表，可以减少带宽的占用。此外，还自动限制这些部分更新的传播，只将其传递给需要的路由器，因此，EIGRP 消耗的带宽比 IGRP 少很多。这种行为也不同于链路状态路由协议，后者将更新发送给区域内的所有路由器。

3. 支持多种网络层协议

EIGRP 使用协议相关模块来支持 IPv4、IPv6、Apple Talk 和 IPX 协议，以满足特定网络层的需求。

4. 使用组播和单播

EIGRP 在路由器之间通信时使用的是组播和单播，而不是广播，因此终端站不受路由更新和查询的影响。EIGRP 使用的组播地址是 224.0.0.10。

5. 支持变长子网掩码

EIGRP 是一种无类路由协议，它通告每个目标网络的网络地址和子网掩码，支持不连续子网和变长子网掩码（VLSM）。

6. 无缝连接数据链路层协议和拓扑结构

不像 OSPF，EIGRP 不要求对 OSI 参考模型的 2 层协议做特别的配置。OSPF 对不同的 2 层协议要做不同配置，如以太网和帧中继。EIGRP 能够有效地工作在 LAN 和 WAN 中，而且 EIGRP 保证网络不会产生环路（loop-free）。

7. 配置简单

使用 EIGRP 组建网络时，路由器配置非常简单，它没有复杂的区域设置，也无须针对不同网络接口类型实施不同的配置方法。配置 EIGRP 只使用 router eigrp 命令在路由器上启动 EIGRP 路由进程，然后再使用 network 命令指定路由器连接的网段即可。

8.1.3 EIGRP 与 OSPF 协议的比较

定时发送 Hello 报文。运行 EIGRP 的路由器之间必须通过定时发送 Hello 报文来维持邻居关系，这种邻居关系即使在拨号网络上，也需要定时发送 Hello 报文，这样，在按需拨号的网络上，无法确定这是有用的业务报文，还是 EIGRP 发送的定时查询报文，从而可能误触发按需拨号网络发起连接，尤其在备份网络上，会引起不必要的麻烦。所以，一般运行 EIGRP 的路由器，在拨号备份端口还须配置 Dialer list 和 Dialer group，以便过滤不必要的

报文，或者运行TRIP，这样做会增加路由器运行的开销。而OSPF可以提供对拨号网络按需拨号的支持，只用一种路由协议就可以满足各种专线或拨号网络应用的需求。

EIGRP的无环路计算和收敛速度是基于分布式的DUAL算法的，这种算法的计算过程实际上是将不确定的路由信息散播（向邻居发query报文），得到所有邻居的确认后（reply报文）再收敛的过程，邻居在不确定该路由信息可靠性的情况下又会重复这种散播，因此，某些情况下可能会出现该路由信息一直处于活动状态（这种路由被称为活动路由栈），并且如果在活动路由的这次DUAL计算过程中出现到该路由的后继（successor）的测量发生变化的情况，就会进行多重计算，这些都会影响DUAL的收敛速度。而OSPF算法则没有这种问题，所以从收敛速度上看，虽然整体相近，但在某种特殊情况下，EIGRP还存在不理想的收敛结果。

一直以来，EIGRP是Cisco公司的私有协议。直到2013年3月，Cisco公司才公开EIGRP的技术文档。Cisco公司是该协议的发明者和唯一具备该协议解释和修改权的厂商。如果要支持EIGRP，需向Cisco公司购买相应版权，并且Cisco公司修改该协议时没有义务通知任何其他厂家和使用该协议的用户。而OSPF是开放的协议，是IETF组织公布的标准。世界上所有的网络设备厂商都支持该协议，所以它的互操作性和可靠性由于公开而得到保障，并且在众多的厂商支持下，该协议也会不断完善。

8.2 EIGRP的工作原理

EIGRP的关键技术主要包括：可靠传输协议（Reliable Transport Protocol，RTP）、协议相关模块（Protocol-Dependent Module，PDM）、邻居的发现/恢复（Neighbor Discovery/Recovery）技术、扩散更新算法（Diffusing Update ALgorithm，DUAL）、DUAL有限状态机（Finite State Machine，FSM）等。

8.2.1 可靠传输协议

可靠传输协议负责EIGRP数据包的按顺序（可靠）发送和接收，这一个可靠的保障措施是通过Cisco私有的可靠组播（Reliable Multicast）算法来实现的，使用组播地址224.0.0.10。当某个邻居接收到这个可靠的组播数据包时，就会以一个单播（Unicast）数据包作为确认。每个确认数据包都包含发送方分配的1个序列号，发送方每发送1个数据包，这个序列号就递增1。另外，发送方也会把从目标路由器接收到的数据包的序列号放到这个要发送的数据包里。在某些情况下，RTP也可以使用无须确认的不可靠的数据包，这种不可靠的数据包中不包含序列号。EIGRP第一次传输数据时都采用组播形式，重传数据时都采用单播。

8.2.2 扩散更新算法的相关术语

扩散更新算法为EIGRP提供的路由收敛时间有可能是各种动态路由协议中最快的。DUAL提供无环路径、无环备用路径、快速收敛和限定更新等功能。DUAL涉及以下7个相关术语。

1. 后继路由器

后继路由器（Successor）是指用于转发数据包的一台相邻路由器，该路由器是通向目的

网络的开销最低的路由。后继路由器的 IP 地址显示在路由表条目中，紧随单词 via。

2. 可行距离

可行距离(Feasible Distance,FD)是计算出的通向目的网络的最低度量。FD 是路由表条目中所列的度量，就是括号内的第二个数字。与其他路由协议中的情况一样，它也称为路由度量。

3. 可行后继路由器

可行后继路由器(Feasible Successor,FS)是指一个邻居，它有一条通向后继路由器连通的同一个目的网络的无环备用路径，并且满足可行性条件。

在拓扑变化时，DUAL 之所以收敛速度快，是因为它可以使用通向其他路由器的备用路径，这些路由器称为可行后继路由器。使用备用路径不需要重新计算 DUAL。

4. 可行性条件

要成为可行后继路由器，必须首先满足可行性条件(Feasible Condition,FC)。当邻居通向一个网络的报告距离(Reported Distance,RD)比本地路由器通向同一个目的网络的可行距离短时，即符合了可行性条件(Feasible Condition,FC)。

5. 报告距离

报告距离(Reported Distance,RD)是 EIGRP 邻居通向相同目的网络的可行距离。报告距离是路由器向邻居报告的、有关自身通向该网络的开销的度量。

6. 被动路由

被动路由(Passive Route)表示路由器当前有一个合法后继，并且 EIGRP 工作正常。在路由器上使用 show ip eigrp top 命令可以查看 eigrp 的拓扑图，其中路由条目前面的字母"P"就表示该路由当前为被动路由。

7. 主动路由

主动路由(Gratuitous Route)表示路由器已经失去了它的后继，它没有任何可用的可行后继，并且当前该路由器正在主动搜寻替代的路由，以实现收敛。

8.2.3 实现路由快速收敛的关键

EIGRP 实现路由快速收敛的关键有两点：首先，EIGRP 路由器维持了一个所有邻居的路由副本，使用这个副本可以计算出自己到达远程网络的开销，如果最佳的路径不可用了，它只需简单地查询本地拓扑表中的内容，并从中选择出最佳的可替代路由；其次，当它本地的拓扑表中也没有可代替的路由时，EIGRP 路由器会很快向邻居求助，请求更新路由。对其他路由器的依赖和对它们提供的信息的利用，就是 DUAL 的"扩散"特性。

8.2.4 路由计算方法

EIGRP 计算一条主路由(最佳路由)和一条备份路由，并放在拓扑表(Topology Table)中。EIGRP 最多支持 16 条链路。它可以支持多种路由类型：内部、外部(非 EIGRP)和汇总路由。

1. EIGRP 度量的 5 个标准

EIGRP 使用复合度量值，计算时涉及网络的 5 种不同的状态参数。

(1) 带宽(bandwidth)。

EIGRP 带宽的计算方法是用 10 的 7 次方除以源和目标之间最低的带宽(以 kb/s 为单

位)，然后再乘以256。

(2) 延迟(delay)。

接口的累积延迟乘以256，单位是10μs。

(3) 可靠性(reliability)。

根据平均无故障工作时间而确定的源和目的之间的可靠性的值。

(4) 负载(loading)。

根据包速率和接口配置带宽确定的源和目的之间的最小的负载值。

(5) 最大传输单元(MTU)。

MTU是路径中最大的传输单元。MTU包含在EIGRP的路由更新里，但是一般不参与EIGRP度量的运算。

2. EIGRP度量值的计算公式

默认情况下，EIGRP度量值(Metric)的计算公式简化为：

$$\text{Metric}=[K1*\text{带宽}+K3*\text{延迟}]$$

如果不能忽略可靠性和负载这两个重要因素，则计算度量值时应使用以下复合公式：

$$\text{Metric}=[K1*\text{带宽}+(K2*\text{带宽})/(256-\text{负载})+K3*\text{延迟}]*[K5/(\text{可靠性}+K4)]$$

默认情况下，K1和K3的值都设为1，而K2、K4和K5的值都设为0。因此，在默认情况下，即在仅考虑带宽和延迟这两个因素时，计算公式可以简化为第一个公式。

在以上公式中，K1、K2、K3的值依次为带宽、负载、延迟的权重，而K4和K5的值则是可靠性的权重。

如果计算得到的Metric值不为整数，则将自动取整。例如，计算结果为8501.39，取整后为8501。

在路由器配置模式下，可以通过修改权重(K值)来改变EIGRP度量值的计算公式。具体地说，修改权重(K值)的命令如下：

```
metric weight tos K1 K2 K3 K4 K5
```

在以上公式中，tos的取值必须设置为0。注意，EIGRP要求两台路由器的每个K值都必须相同，才能成为邻居。Cisco公司建议，K1、K2、K3、K4和K5的值最好不要修改，因为当这些参数不为默认值时，会使路由器计算度量值时除了关注带宽和延迟，也关注接口的负载和可靠性。而负载和可靠性是随着时间不停地变化的，这将可能导致EIGRP重新泛洪拓扑数据，还可能导致路由器不停地选择不同的路由，使得路由器工作不稳定。

8.2.5 EIGRP数据包

EIGRP使用多种类型的数据包，这些数据包通过IP头部信息里的协议号88来标识：在EIGRP中，共使用5种类型的数据包，分别为Hello、Update、Query、Reply、Ack。下面介绍每种数据包的功能。

1. 问候(Hello)数据包

问候(Hello)数据包是用来发现和维护EIGRP邻居关系的，目标地址为224.0.0.10，邻居收到Hello数据包后不需要确认。Hello包一般是每隔5s组播1次(要随机减去1个很小的时间，防止同步)。

2. 更新(Update)数据包

更新(Update)数据包发给邻居的路由表,通过组播发送 Update 数据包,邻居收到后必须回复确认消息。EIGRP 的 Update 包是非周期性发送的。

3. 查询(Query)数据包

查询(Query)数据包用来查询路由表,当路由信息丢失并且没有备用路由时,使用 Query 数据包向邻居查询,邻居必须回复确认。

4. 回复(Reply)数据包

回复(Reply)数据包是对邻居发送的 Query 数据包的回复,也需要邻居回复确认。

5. 确认(Ack)数据包

确认(Ack)数据包是对收到的数据包的确认,告诉邻居自己已经收到数据包了,收到 Ack 后,就不需要再对 Ack 做回复,因为这是没有意义的,并且可能造成死循环。

由以上介绍可以看出,5 种数据包中,Update、Query、Reply 在对方收到后,都需要回复确认,这些数据包是可靠的,回复是发送 Ack;而 Hello 和 Ack 是不需要回复的,因此被认为不可靠。

8.2.6 修改计时器的方法

在多点(multipoint)、X.25、帧中继(Frame Relay,FR)、ATM 接口和 ISDN PRI 接口上,Hello 包的发送间隔时间是 60s。

可以在接口配置模式下修改该接口的 Hello 包默认的发送间隔时间,命令格式为:

```
ip hello - interval eigrp
```

当一个路由器收到从邻居发来的 Hello 包的时候,这个 Hello 包中包含了一个有效时间,这个有效时间是指路由器等待后续 Hello 包的最大时间。如果在超出这个有效时间后仍然没有收到邻居发来的后续 Hello 包,那么这个邻居就会被宣告为不可达,并通知 DUAL 这个邻居已丢失。

默认情况下,有效时间是 Hello 包发送间隔时间的 3 倍,可以在接口配置模式下修改这个默认的有效时间,命令格式为:

```
ip hold - time eigrp
```

EIGRP 邻居信息都记录在邻居表(Neighbor Table)中,在特权模式下,可以使用 show ip eigrpneighbors 命令查看 EIGRP 的邻居。

8.2.7 解决环路问题

与其他动态路由算法一样,EIGRP 也要解决环路问题。EIGRP 解决环路问题的方法有水平分割(Split Horizon)和路由的毒性逆转(Poison Reverse)。

1. 水平分割

水平分割是指永远不会在同一个接口下通告一条从该接口学到的路由信息。发送查询请求时,会引起水平分割,如当一个路由器查询一条未知网段的去向时,它会向每个邻居发送查询,处于该网段的继承者会返回查询给该路由器,而该路由器会反馈一个查询结果给其他邻居,但不会再次告诉那个继承者走这个网段要经过自己。

2. 路由的毒性逆转

接收到来自邻居某接口的路由信息后,路由器会从该接口通告刚才学到的路由为不可达。当两台路由器进行邻居初始化时,它们会互相以最大的度量(metric)值通告刚才学到的路由信息(路由中毒)。当拓扑发生改变时,会暂时关闭水平分割和毒性逆转,重新学习拓扑结构。

8.2.8 DUAL 有限状态机

EIGRP 的核心就是 DUAL 和 EIGRP 的路由计算引擎。这项技术准确的名称是 DUAL 有限状态机(Finite State Machine,FSM)。

DUAL 有限状态机包含用于在 EIGRP 网络中计算和比较路由的所有算法。DUAL 有限状态机如图 8-1 所示。

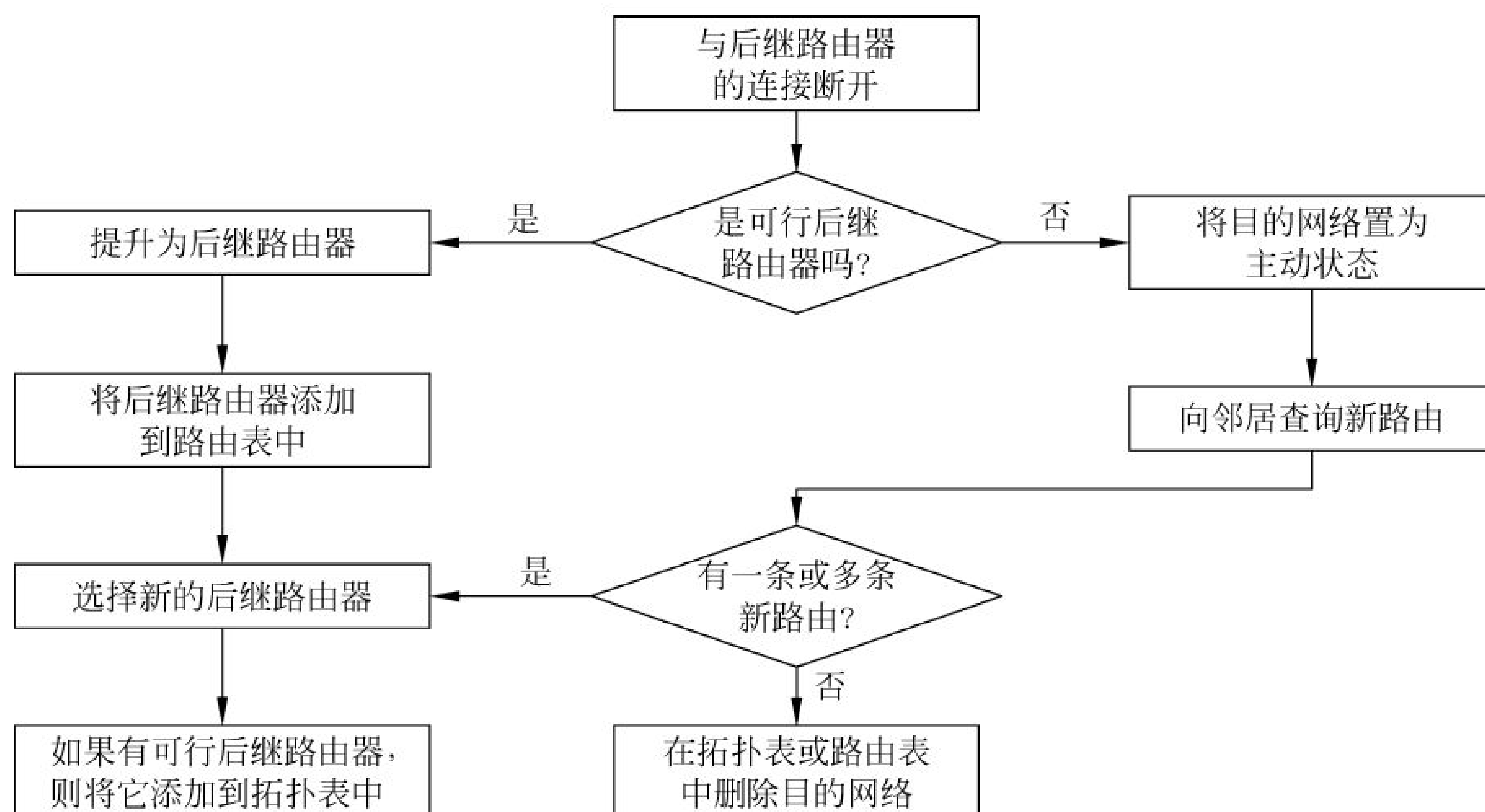


图 8-1 DUAL 有限状态机

总结 DUAL 如下:

(1) 记录邻居通告给本路由器的所有路由,并写入拓扑表。

(2) 选择 FD 最小的成为继任路由,并写入 IP 路由表。

(3) 根据路由 AD 小于最优路由 FD 的原则,选择可行继任路由。

(4) 最优路由故障,则检查拓扑表。若存在可行继任路由,则可以直接使用它作为新的最优路由,该路由保持在被动(Passive)状态;若不存在可行继任路由,则向所有的 EIGRP 邻居查询该路由,该路由变为激活(Active)状态。如果本路由器未收到所有查询(Query)的回复(Reply)报文,将无法计算新的路由,该路由就会长时间处于激活(Active)状态,该状态称为黏滞于激活状态(Stuck in Active,SIA),默认时间为 3min,iOS 12.3 以后的版本对 SIA 状态的处理进行了改进,即在激活计时器(Active Timer)90s 的计时结束后发送一个黏滞于激活状态的查询(SIA Query)报文,以确认与此邻居之间的连通性,若收到连通性确认报文,但未收到回复(Reply)报文,则 90s 后再重新发送一次 SIA Query 并等待确认,连续 7 次之后,将不再发送该报文,在激活计时器 3min 计时结束后,就会把该路由删除。

正常状况下,EIGRP 的每条路由都处于被动路由的状态下,在产生一个输入事件的时

候，路由器会重新评估一条路由的可行后继列表。这些事件可以是直连链路的代价或状态发生变化，收到一个查询、答复和更新等。

路由器重新评估的第一步是进行本地计算（Local Computation），也就是对所有的可行后继路由器重新计算。如果发现可用可行后继，路由将继续保持被动状态。如果没有一台可用的可行后继，则路由条目变成激活（Active）状态，并进行扩散计算。

路由器通过向所有的邻居发送查询开始扩散计算，邻居收到查询后会进入本地计算阶段，如果邻居有到达目的网络的一条或多条可行后继，则答复请求，请求中包括到达目的网络。如果没有可行后继，邻居就会继续进行扩散计算。

在一个路由器开始进行扩散计算的时候，会有一个被设置为3min的扩散计时器，如果在扩散计时器超时之后还没有收到回复，该条路由就会被挂起（Stuck In Active，SIA），90s后再次发送查询报文，如果没有答复，邻居路由器就会从邻居表中被删除。

8.3 EIGRP的配置和管理

8.3.1 EIGRP配置命令

虽然EIGRP的工作原理比较复杂，但是它的配置和管理方法却非常简单，与RIP的配置命令很相似。各个配置命令及功能说明如下。

1. router eigrp 进程编号 ID

router eigrp 进程编号 ID 是一个全局配置命令，用于启动EIGRP。其中的参数进程编号ID的取值范围为1～65 535，用作对EIGRP进程统一编号。这个进程编号非常重要，因为在同一个EIGRP域内，所有的路由器都必须使用相同的ID编号。

2. network 网络地址

EIGRP中的network命令与RIP中的network命令功能相同。一旦用network命令指定了网络地址，路由器上任何符合network命令中的网络地址的接口都将被启用，可以发送和接收EIGRP更新信息。

3. show ip eigrp neigbors

在特权模式下使用show ip eigrp neigbors命令可以查看邻居表，并检验EIGRP是否已经与邻居建立了邻接关系。对于每台路由器，我们都可以看到邻接路由器的IP地址和通向这个邻居的接口。

4. show ip protocols

与查看其他路由协议参数相似，也可以在特权模式下使用show ip protocols命令来检验EIGRP是否已经启用。对于不同的路由协议，show ip protocols返回的结果略有不同。

5. show ip route

与查看其他路由协议产生的路由表相似，也可以在特权模式下使用show ip route命令来检验EIGRP生成的路由表，这也是检验EIGRP以及路由器的其他功能是否正确配置的另一种有效的方法。

6. show interface

在特权模式下，使用show interface命令可以检查路由器各个接口的带宽、延迟、可靠性和负载的实际值。

7. bandwidth 带宽值

在接口配置模式下,可以使用 bandwidth 带宽值修改接口的带宽度量值。在大多数串行链路上,带宽度量默认值为 1544kb/s。但是,如果链路的实际带宽与默认带宽不符,就需要对带宽度量值进行修改,以适应实际的带宽。反之,在接口配置模式下,使用命令 no bandwidth 可以将接口的带宽度量值恢复为默认值。

8.3.2 EIGRP 调试命令

配置 EIGRP 时,常用的调试命令及功能介绍如下。

```
show run | begin router eigrp                     //查看配置文件中 eigrp 的配置命令
show ip protocols                                 //查看当前路由器运行的 eigrp 协议状态
show ip route summary                             //查看 eigrp 路由汇总状态
show ip eigrp neighbors                           //查看 eigrp 邻居状态
show ip eigrp interface                           //查看各个运行 eigrp 的接口状态
show ip eigrp interface detail                    //查看各个运行 eigrp 的接口详细状态
show ip route eigrp                               //查看 eigrp 协议学习到的路由表
show ip eigrptopology                             //查看 eigrp 的拓扑表
show ip eigrptopology all - links                 //查看 eigrp 完整的拓扑表
show ip eigrptopology 10.1.1.0 255.255.255.0      //查看指定的某个网络参数信息
debug eigrp 数据包 s                               //调试 eigrp 的查询包
debug eigrp fsm                                   //调试 eigrp 的 DUAL 信息
```

8.3.3 EIGRP 配置实例

下面以图 8-2 所示的网络环境为例,介绍 EIGRP 的配置方法。

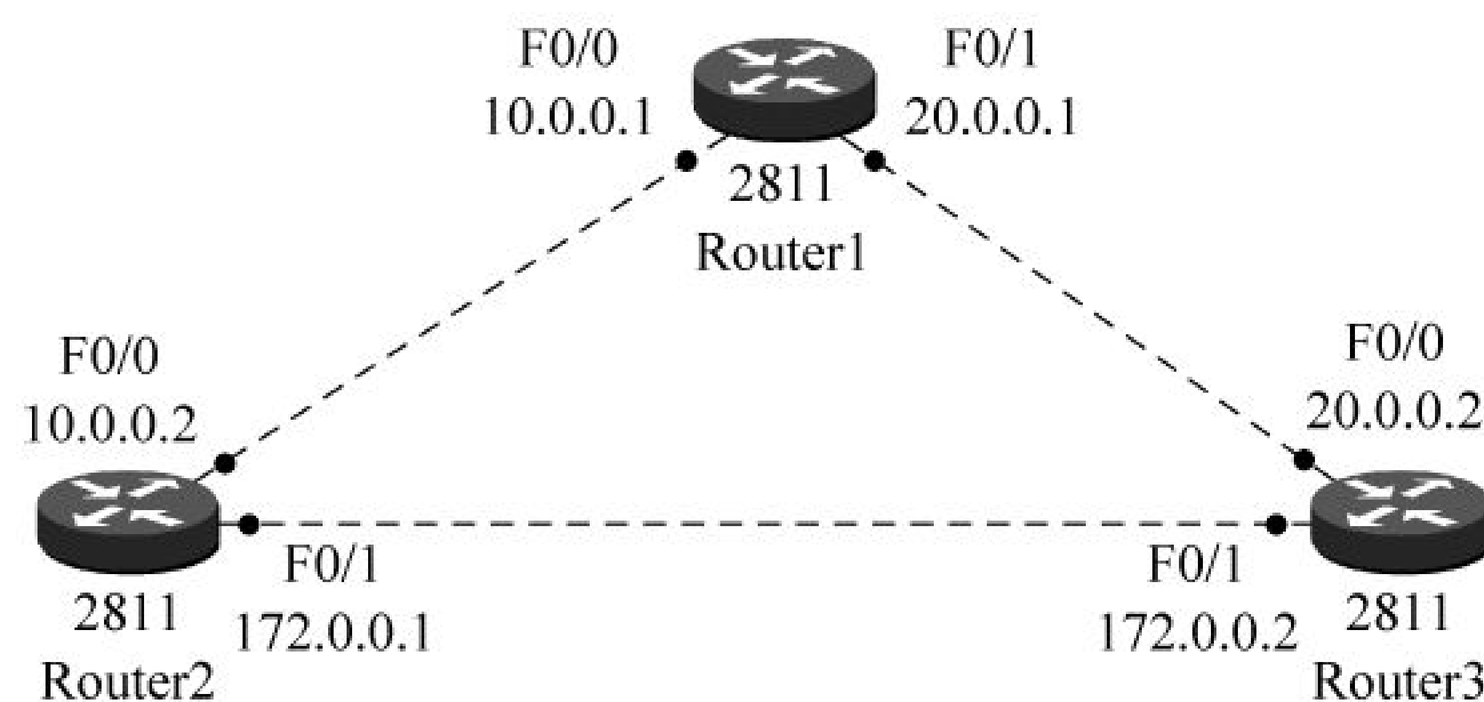


图 8-2 EIGRP 配置的网络环境

第一步,请按照图 8-2 分别给 3 个路由器的各个接口配置 IP 地址和子网掩码。接着,对路由器 Router1 配置 EIGRP,具体的操作命令如图 8-3 所示。

```
Router1(config)#router eigrp 100
Router1(config-router)#no auto-summary
Router1(config-router)#network 10.0.0.0
Router1(config-router)#network 20.0.0.0
Router1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
Router1#
```

图 8-3 对路由器 Router1 配置 EIGRP

在图 8-3 中，第 1 行命令 router eigrp 100 的作用是启动一个 EIGRP 进程，其中的 100 是自治系统号；第 2 行命令 no auto-summary 的作用是关闭自动汇总功能；第 3、4 行命令 network 的作用是向邻居的路由器通告 10.0.0.0 和 20.0.0.0 这两个网段。

同理，需要对路由器 Router2 配置 EIGRP，具体的操作命令如图 8-4 所示。

```
Router2(config)#router eigrp 100
Router2(config-router)#no auto-summary
Router2(config-router)#network 10.0.0.0
Router2(config-router)#network 172.0.0.0
Router2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
Router2#
```

图 8-4　对路由器 Router2 配置 EIGRP

在图 8-4 中，第 1 行命令 router eigrp 100 的作用是启动一个 EIGRP 进程。注意，这里的路由器 Router2 自治系统号必须设置为与路由器 Router1 的自治系统号完全相同，即也要设置为 100；第 2 行命令 no auto-summary 的作用是关闭自动汇总功能；第 3、4 行命令 network 的作用是向邻居的路由器通告 10.0.0.0 和 172.0.0.0 这两个网段。

最后，需要对路由器 Router3 配置 EIGRP，具体的操作命令如图 8-5 所示。

```
Router3(config)#router eigrp 100
Router3(config-router)#no auto-summary
Router3(config-router)#network 20.0.0.0
Router3(config-router)#network 172.0.0.0
Router3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
Router3#
```

图 8-5　对路由器 Router3 配置 EIGRP

在图 8-5 中，第 1 行命令 router eigrp 100 的作用同样是启动一个 EIGRP 进程。注意，这里的路由器 Router3 自治系统号也必须设置为与路由器 Router1 的自治系统号完全相同，即也要设置为 100；第 2 行命令 no auto-summary 的作用是关闭自动汇总功能；第 3、4 行命令 network 的作用是向邻居的路由器通告 20.0.0.0 和 172.0.0.0 这两个网段。

至此，3 个路由器的 EIGRP 都已经配置完成了。

下面进一步介绍验证 EIGRP 配置结果的有关命令。

首先，用命令 show ip route 查看路由表，结果如图 8-6 所示。

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - 1
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS :
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    20.0.0.0/8 is directly connected, FastEthernet0/1
D    172.0.0.0/16 [90/30720] via 10.0.0.2, 01:14:23, FastEthernet0/0
                  [90/30720] via 20.0.0.2, 01:12:22, FastEthernet0/1
Router1#
```

图 8-6　查看路由表

在图 8-6 中,倒数第 3 行和倒数第 2 行以字母 D 带头的两行信息,正是配置成功的 EIGRP 路由。它表明到达网段 172.0.0.0/16 有两条路由:一条路由途经下一跳地址10.0.0.2;另一条路由途经下一跳地址 20.0.0.2。

此时如果用命令 show ip route eigrp,则返回的路由信息更加简洁,仅显示 EIGRP 路由,如图 8-7 所示。

```
Router1#show ip route eigrp
D    172.0.0.0/16 [90/30720] via 10.0.0.2, 01:35:02, FastEthernet0/0
                  [90/30720] via 20.0.0.2, 01:33:01, FastEthernet0/1
Router1#
```

图 8-7 查看 EIGRP 路由

接着,可以用命令 show ip protocols 查看路由协议信息,结果如图 8-8 所示。

```
Router1#show ip protocols

Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
     10.0.0.0
     20.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.2        90            1849108
    20.0.0.2        90            1963414
  Distance: internal 90 external 170

Router1#
```

图 8-8 查看路由协议信息

EIGRP 共有 3 张表,除了路由表外,还有拓扑表和邻居表。查看拓扑表的命令是 show ip eigrp topology,执行结果如图 8-9 所示。

```
Router1#show ip eigrp topology
IP-EIGRP Topology Table for AS 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.0.0/8, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 20.0.0.0/8, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 172.0.0.0/16, 2 successors, FD is 30720
         via 20.0.0.2 (30720/28160), FastEthernet0/1
         via 10.0.0.2 (30720/28160), FastEthernet0/0
Router1#
```

图 8-9 查看拓扑表

查看邻居表的命令是 show ip eigrp neighbors。这条命令可以在配置的过程中使用，用作查看相邻的两台 EIGRP 路由器是否成功地建立了邻居关系。这条命令执行的结果如图 8-10 所示。从显示的信息中可以看到邻居的接口 IP 地址、该邻居相连的接口和计时器信息等内容。

```
Router1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address          Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)         Cnt Num
0   20.0.0.2         Fa0/1          10   00:00:27  40     1000  0   3
1   10.0.0.2         Fa0/0          14   00:00:27  40     1000  0   3

Router1#
```

图 8-10 查看邻居表

8.4 支持 IPv6 的 EIGRP

8.4.1 支持 IPv6 的 EIGRP 的特点

在 IPv6 环境下，EIGRP 的运行过程和在 IPv4 环境下的运行过程一样。EIGRP 使用新的类型卡度值（Type-Length-Value，TLV）来携带 IPv6 路由信息。

支持 IPv6 的 EIGRP 具有以下不同于 IPv4 EIGRP 的新特征：

（1）EIGRP IPv6 进程直接运行在接口上，并没有类似 IPv4 下的 network 命令。只要接口下启用了 EIGRP，不需要在路由器模式下配置任何命令，EIGRP 就可以运行。

（2）EIGRP 需要路由器 ID 号，这个 ID 号是 IPv4 地址。

（3）接口在被动（Passive）模式下不需要配置 IPv6 进程。

（4）EIGRPv6 进程可以关闭。

8.4.2 配置 EIGRPv6 的命令

```
ipv6 unicast - routing              //启用 IPv6 单播路由功能
ipv6 router eigrp 自治区编号          //在指定编号的整个自治区内启用 EIGRPv6 进程
router - id ID 号                    //配置路由器 ID 号
ipv6 eigrp 自治区编号                 //在接口上启用 EIGRPv6 进程
ipv6 enable                         //在接口上启用 IPv6
```

8.4.3 测试 EIGRPv6 的命令

```
show ipv6 protocols                 //查看当前运行的路由协议
show ipv6 route                     //查看完整的路由表
show ipv6 route eigrp               //仅查看路由表中的 EIGRP 路由
show ipv6 eigrp neighbors           //查看 eigrp 协议的邻居表
show ipv6 eigrp topology            //查看 eigrp 协议的拓扑表
show ipv6 eigrp traffic             //查看 eigrp 收发数据包的次数
show ip eigrptopology               //查看 eigrp 的拓扑表
ping ipv6 地址                       //测试网络的连通性
```

8.4.4 EIGRPv6 的配置实例

下面以图 8-11 所示的 IPv6 网络环境为例，介绍 EIGRPv6 的配置过程。

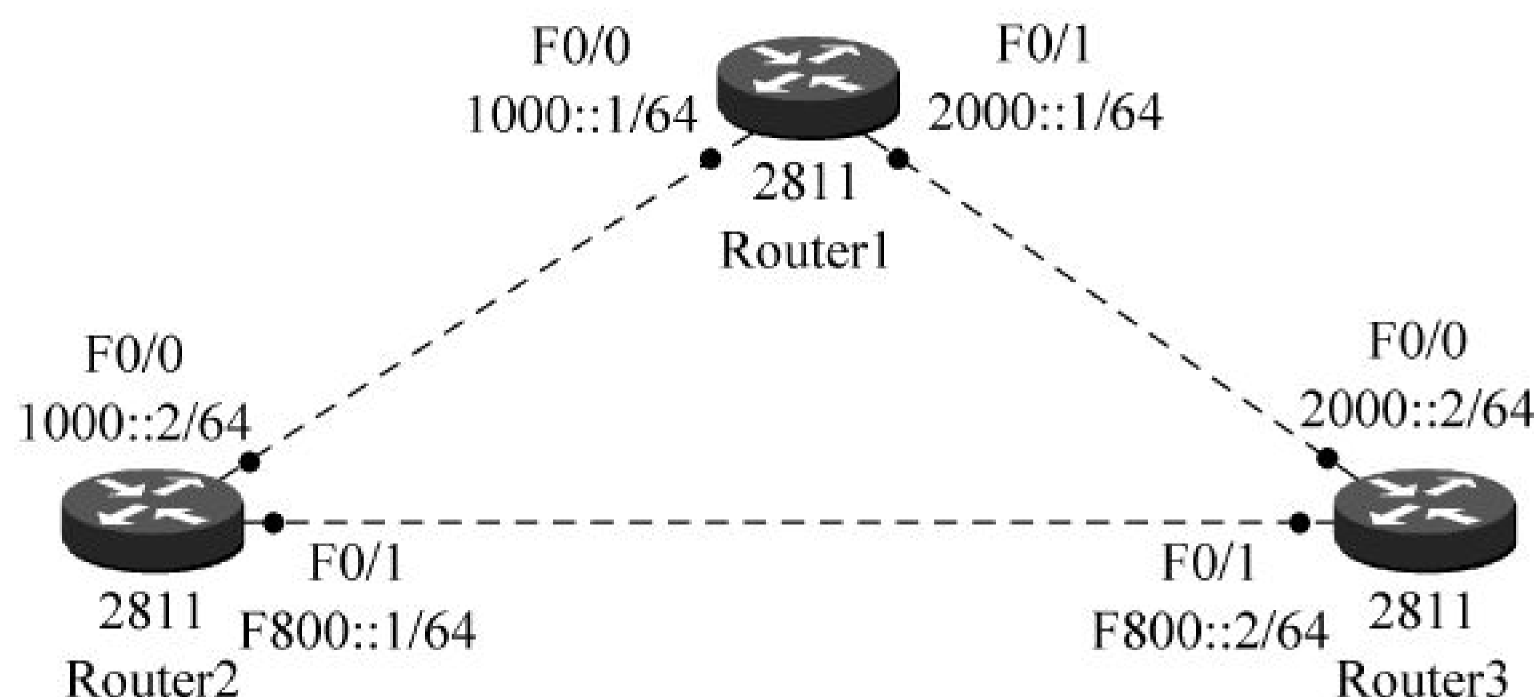


图 8-11 EIGRPv6 的配置环境

1. 配置路由器 Router1 的 EIGRPv6

配置路由器 Router1 的 EIGRPv6 的具体操作命令如图 8-12 所示。

```
1  Router1(config)#ipv6 unicast-routing
2  Router1(config)#ipv6 router eigrp 100
3  Router1(config-rtr)#router-id 1.1.1.1
4  Router1(config-rtr)#no shutdown
5  Router1(config-rtr)#exit
6  Router1(config)#interface f0/0
7  Router1(config-if)#ipv6 address 1000::1/64
8  Router1(config-if)#ipv6 enable
9  Router1(config-if)#ipv6 eigrp 100
10 Router1(config-if)#exit
11 Router1(config)#interface f0/1
12 Router1(config-if)#ipv6 address 2000::1/64
13 Router1(config-if)#ipv6 enable
14 Router1(config-if)#ipv6 eigrp 100
15 Router1(config-if)#end
16 %SYS-5-CONFIG_I: Configured from console by console
17 Router1#
```

图 8-12 配置路由器 Router1 的 EIGRPv6

在图 8-12 中，每行命令的作用说明如下。

第 1 行命令 ipv6 unicast-routing 的作用是启用 IPv6 单播路由功能。

第 2 行命令 ipv6 router eigrp 100 的作用进入路由协议配置模式，命令执行后，提示符变为第 3 行开头的(config-rtr)，并在指定编号的整个自治区内启用 EIGRPv6 进程，本例中，自治区编号设置为 100，自治区编号的取值范围是 1～65 535。

第 3 行命令 router-id ID 号的作用是配置路由器 ID 号，通常将 ID 号设置为路由器接口的 IPv4 地址，以方便识别，在本例中设置为 1.1.1.1。

第 4 行命令 no shutdown 的作用是激活进程。

第 5 行命令 exit 的作用是返回全局配置模式。

第 6 行命令 interface f0/0 的作用是进入接口配置模式，提示符变为(config-if)，并指定需要配置的接口为快速以太网接口 Fast Ethernet 0/0。

第 7 行命令 ipv6 address 的作用是为接口配置 IPv6 地址。

第 8 行命令 ipv6 enable 的作用是在接口上启用 IPv6。

第 9 行命令 ipv6 eigrp 自治区编号的作用是在接口上启用 IPv6 进程，这条命令中的自治区编号必须与第 2 行的 ipv6 router eigrp 自治区编号中的自治区编号相同。

第 10 行命令 exit 的作用是返回全局配置模式。

第 11～14 行命令的作用与第 6～9 行命令的作用相同，这里不再重复。

第 15 行命令 end 的作用是直接回到特权模式。

2. 配置路由器 Router2 的 EIGRPv6

同理，可以继续配置路由器 Router2 的 EIGRPv6，具体操作命令如图 8-13 所示。

```
1  Router2(config)#ipv6 unicast-routing
2  Router2(config)#ipv6 router eigrp 100
3  Router2(config-rtr)#router-id 2.2.2.2
4  Router2(config-rtr)#no shutdown
5  Router2(config-rtr)#exit
6  Router2(config)#interface f0/0
7  Router2(config-if)#ipv6 address 1000::2/64
8  Router2(config-if)#ipv6 enable
9  Router2(config-if)#ipv6 eigrp 100
10 Router2(config-if)#exit
11 Router2(config)#
12 %DUAL-5-NBRCHANGE: IPv6-EIGRP 100: Neighbor FE80::205:5EFF:
13 et0/0) is up: new adjacency
14 Router2(config)#interface f0/1
15 Router2(config-if)#ipv6 address F800::1/64
16 Router2(config-if)#ipv6 enable
17 Router2(config-if)#ipv6 eigrp 100
18 Router2(config-if)#end
```

图 8-13　配置路由器 Router2 的 EIGRPv6

在图 8-13 中，每行命令的作用说明如下。

第 1 行命令 ipv6 unicast-routing 的作用是启用 IPv6 单播路由功能。

第 2 行命令 ipv6 router eigrp 100 的作用是进入路由协议配置模式，命令执行后，提示符变为第 3 行开头的(config-rtr)，并在指定编号的整个自治区内启用 EIGRPv6 进程，本例中，自治区编号设置为 100，自治区编号的取值范围是 1～65 535。

第 3 行命令 router-id ID 号的作用是配置路由器 ID 号，通常将 ID 号设置为路由器接口的 IPv4 地址，以方便识别，在本例中设置为 2.2.2.2。

第 4 行命令 no shutdown 的作用是激活进程。

第 5 行命令 exit 的作用是返回全局配置模式。

第 6 行命令 interface f0/0 的作用是进入接口配置模式，提示符变为(config-if)，并指定需要配置的接口为快速以太网接口 Fast Ethernet 0/0。

第 7 行命令 ipv6 address 的作用是为接口配置 IPv6 地址。

第 8 行命令 ipv6 enable 的作用是在接口上启用 IPv6。

第 9 行命令 ipv6 eigrp 自治区编号的作用是在接口上启用 IPv6 进程，这条命令中的自治区编号必须与第 2 行的 ipv6 router eigrp 自治区编号中的自治区编号相同。

第 10 行命令 exit 的作用是返回全局配置模式。

在图 8-13 中，其余各行命令的作用与前面所述的 Router1 的 EIGRPv6 配置命令作用相似，这里不再重复。

3. 配置路由器 Router3 的 EIGRPv6

同理,配置路由器 Router3 的 EIGRPv6 的具体操作命令如图 8-14 所示。

```
Router3(config)#ipv6 unicast-routing
Router3(config)#ipv6 router eigrp 100
Router3(config-rtr)#router-id 3.3.3.3
Router3(config-rtr)#no shutdown
Router3(config-rtr)#exit
Router3(config)#interface f0/0
Router3(config-if)#ipv6 address 2000::2/64
Router3(config-if)#ipv6 enable
Router3(config-if)#ipv6 eigrp 100
Router3(config-if)#exit
Router3(config)#
%DUAL-5-NBRCHANGE: IPv6-EIGRP 100: Neighbor FE80::205:5EFF:
et0/0) is up: new adjacency
Router3(config)#interface f0/1
Router3(config-if)#ipv6 address F800::2/64
Router3(config-if)#ipv6 enable
Router3(config-if)#ipv6 eigrp 100
Router3(config-if)#end
%DUAL-5-NBRCHANGE: IPv6-EIGRP 100: Neighbor FE80::201:96FF:
et0/1) is up: new adjacenc
Router3(config-if)#
```

图 8-14 配置路由器 Router3 的 EIGRPv6 的具体操作命令

至此,3 个路由器的 EIGRPv6 配置完成。

4. 验证 EIGRPv6

1) 查看正在运行的路由协议

在 Router1 的特权模式中用命令 show ipv6 protocols 查看正在运行的路由协议,结果如图 8-15 所示。

```
Router1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static
IPv6 Routing Protocol is "eigrp  100 "
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Interfaces:
    FastEthernet0/0
    FastEthernet0/1
  Redistribution:
    None
  Maximum path: 16
  Distance: internal 90 external 170

Router1#
```

图 8-15 查看正在运行的路由协议

2) 查看邻居表

在 Router1 的特权模式中用命令 show ipv6 eigrp neighbors 查看邻居表,结果如图 8-16 所示。

3) 查看拓扑表

在 Router1 的特权模式中用命令 show ipv6 eigrp topology 查看拓扑表,结果如图 8-17 所示。

```
Router1#show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 100
H   Address               Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                          (sec)          (ms)        Cnt  Num
0   FE80::201:96FF:FE83:8501Fa0/0          12   00:33:00  40     1000  0
1   FE80::201:64FF:FE0E:AB01Fa0/1          11   00:21:49  40     1000  0

Router1#
```

图 8-16 查看邻居表

```
Router1#show ipv6 eigrp topology
IPv6-EIGRP Topology Table for AS 100/ID(1.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 1000::/64, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 2000::/64, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P F800::/64, 2 successors, FD is 30720
         via FE80::201:96FF:FE83:8501 (30720/28160), FastEthernet0/0
         via FE80::201:64FF:FE0E:AB01 (30720/28160), FastEthernet0/1
Router1#
```

图 8-17 查看拓扑表

4）查看路由表

在 Router1 的特权模式中用命令 show ipv6 route 查看路由表，结果如图 8-18 所示。

```
1  Router1#show ipv6 route
2  IPv6 Routing Table - 6 entries
3  Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
4         U - Per-user Static route, M - MIPv6
5         I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
6         O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext
7         ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
8         D - EIGRP, EX - EIGRP external
9  C   1000::/64 [0/0]
10      via ::, FastEthernet0/0
11 L   1000::205:5EFF:FEC4:1E01/128 [0/0]
12      via ::, FastEthernet0/0
13 C   2000::/64 [0/0]
14      via ::, FastEthernet0/1
15 L   2000::205:5EFF:FEC4:1E02/128 [0/0]
16      via ::, FastEthernet0/1
17 D   F800::/64 [90/30720]
18      via FE80::201:96FF:FE83:8501, FastEthernet0/0
19      via FE80::201:64FF:FE0E:AB01, FastEthernet0/1
20 L   FF00::/8 [0/0]
21      via ::, Null0
22 Router1#
```

图 8-18 查看路由表

在图 8-18 中，第 17 行以字母 D 带头的信息就是由 EIGRPv6 生成的前往 IPv6 地址 F800::/64 的路由。

5）查看 IPv6 数据包的收发次数

在 Router1 的特权模式中用命令 show ipv6 eigrp traffic 查看 IPv6 数据包的收发次数，

结果如图 8-19 所示。

```
Router1#show ipv6 eigrp traffic
IPv6-EIGRP Traffic Statistics for process 100
  Hellos sent/received: 765/428
  Updates sent/received: 10/4
  Queries sent/received: 0/0
  Replies sent/received:  0/0
  Acks sent/received:  4/3
  Input queue high water mark 1, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0

Router1#
```

图 8-19　查看 IPv6 数据包的收发次数

从图 8-19 中可以看出，问候(Hello)数据包的发送和接收次数分别是 765 次和 428 次；更新(Update)数据包的发送和接收次数分别是 10 次和 4 次；查询(Query)数据包的发送和接收次数都是 0；回复(Reply)数据包的发送和接收次数都是 0；响应(Ack)数据包的发送和接收次数分别是 4 次和 3 次。

6）测试 IPv6 网络的连通性

在 Router1 的特权模式中用 ping 命令分别测试路由器 Router1 与每个 IPv6 网段的连通性，结果如图 8-20 所示，表明网络的连通性全部正常。

```
Router1#ping 1000::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1000::2, timeout is 2 sec
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping 2000::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000::2, timeout is 2 sec
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping F800::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to F800::2, timeout is 2 sec
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#
```

图 8-20　测试 IPv6 网络的连通性

8.5　本章总结

增强型内部网关路由协议(Enhanced Interior Gateway Routing Protocol，EIGRP)的前身是内部网关路由协议(Interior Gateway Routing Protocol，IGRP)。

IGRP 是由 Cisco 公司于 20 世纪 80 年代中期设计并推出的，同时使用延迟、带宽、可靠

性和负载等因素来确定最佳路由。默认状态下，IGRP 每 90s 发送一次路由更新广播，在 3 个更新周期（即 270s）内如果没有接收到某个路由器发送的更新信息，则会宣布该路由器不可访问。在 7 个周期（即 630s）之后，IGRP 会从路由表中清除该路由。

增强型内部网关路由协议是综合了链路状态算法和距离矢量型路由选择算法的 Cisco 专用协议。EIGRP 采用扩散更新算法（DUAL）实现快速收敛，可以不发送定期的路由更新信息，以减少带宽的占用，支持 Apple Talk、IP、Novell 和 NetWare 等多种网络层协议。自从 EIGRP 路由协议诞生后，IGRP 路由协议就逐渐被淘汰了。

EIGRP 的关键技术主要包括：可靠传输协议（Reliable Transport Protocol，RTP）、协议相关模块（Protocol-Dependent Module，PDM）、邻居的发现/恢复（Neighbor Discovery/Recovery）技术、扩散更新算法（Diffusing Update Algorithm，DUAL）、DUAL 有限状态机（Finite State Machine，FSM）等。

虽然 EIGRP 的工作原理比较复杂，但是它的配置和管理方法却非常简单，与 RIP 的配置命令很相似。各个配置命令及功能说明如下。

1. router eigrp 进程编号 ID

router eigrp 进程编号 ID 是一个全局配置命令，用于启动 EIGRP。其中的参数“进程编号 ID”的取值范围为 1～65 535，用作对 EIGRP 进程统一编号。这个进程编号非常重要，因为在同一个 EIGRP 域内，所有路由器都必须使用相同的 ID 编号。

2. network 网络地址

EIGRP 中的 network 命令与 RIP 中的 network 命令功能相同。一旦用 network 命令指定了网络地址，路由器上任何符合 network 命令中的网络地址的接口都将被启用，可以发送和接收 EIGRP 更新信息。

3. show ip eigrp neigbors

在特权模式下使用 show ip eigrp neigbors 命令可以查看邻居表，并检验 EIGRP 是否已经与邻居建立了邻接关系。对于每台路由器，我们都可以看到邻接路由器的 IP 地址和通向这个邻居的接口。

4. show ip protocols

与查看其他路由协议参数相似，也可以在特权模式下使用 show ip protocols 命令来检验 EIGRP 是否已经启用。对于不同的路由协议，show ip protocols 返回的结果略有不同。

5. show ip route

与查看其他路由协议产生的路由表相似，也可以在特权模式下使用 show ip route 命令来检验 EIGRP 生成的路由表，这也是检验 EIGRP 以及路由器的其他功能是否正确配置的另一种有效的方法。

6. show interface

在特权模式下，使用 show interface 命令可以检查路由器各个接口的带宽、延迟、可靠性和负载的实际值。

7. bandwidth 带宽值

在接口配置模式下，可以使用 bandwidth 带宽值修改接口的带宽度量值。在大多数串行链路上，带宽度量默认值为 1544kb/s。

配置 EIGRP 时，常用的调试命令及功能介绍如下。

```
show run | begin router eigrp                //查看配置文件中 eigrp 的配置命令
show ip protocols                            //查看当前路由器运行的 eigrp 协议状态
show ip route summary                        //查看 eigrp 路由汇总状态
show ip eigrp neighbors                      //查看 eigrp 邻居状态
show ip eigrp interface                      //查看各个运行 eigrp 的接口状态
show ip eigrp interface detail               //查看各个运行 eigrp 的接口详细状态
show ip route eigrp                          //查看 eigrp 协议学习到的路由表
show ip eigrptopology                        //查看 eigrp 的拓扑表
show ip eigrptopology all - links            //查看 eigrp 完整的拓扑表
show ip eigrptopology 10.1.1.0 255.255.255.0//查看指定的某个网络参数信息
debug eigrp 数据包 s                         //调试 eigrp 的查询包
debug eigrp fsm                              //调试 eigrp 的 DUAL 信息
```

支持 IPv6 的 EIGRP 具有以下不同于 IPv4 环境下的新特征：

(1) EIGRP IPv6 进程直接运行在接口上，并没有类似 IPv4 下的 network 命令。只要接口下启用了 EIGRP，不需要在路由器模式下配置任何命令，EIGRP 就可以运行。

(2) EIGRP 需要路由器 ID 号，这个 ID 号是 IPv4 地址。

(3) 接口在被动(Passive)模式下不需要配置 IPv6 进程。

(4) EIGRPv6 进程可以关闭。

配置 EIGRPv6 的命令及功能小结如下。

```
ipv6 unicast - routing                       //启用 IPv6 单播路由功能
ipv6 router eigrp 自治区编号                 //在指定编号的整个自治区内启用 EIGRPv6 进程
router - id ID 号                            //配置路由器 ID 号
ipv6 eigrp 自治区编号                        //在接口上启用 EIGRPv6 进程
ipv6 enable                                  //在接口上启用 IPv6
```

配置 EIGRPv6 时，常用的测试命令及功能归纳如下。

```
show ipv6 protocols                          //查看当前运行的路由协议
show ipv6 route                              //查看完整的路由表
show ipv6 route eigrp                        //仅查看路由表中的 EIGRP 路由
show ipv6 eigrp neighbors                    //查看 eigrp 协议的邻居表
show ipv6 eigrp topology                     //查看 eigrp 协议的拓扑表
show ipv6 eigrp traffic                      //查看 eigrp 收发数据包的次数
show ip eigrptopology                        //查看 eigrp 的拓扑表
ping ipv6 地址                               //测试网络的连通性
```

复习思考题

1. 什么是 IGRP? IGRP 目前还在使用吗?
2. 什么是 EIGRP? EIGRP 与 IGRP 有何区别?
3. EIGRP 仍然是 Cisco 公司的私有协议吗?
4. EIGRP 的优点是什么?
5. EIGRP 与 OSPF 相比有什么不同?
6. 请给出 EIGRP 度量的复合计算公式，并说明公式中每个参数的含义。

7. EIGRP 包括哪些数据包？每种 EIGRP 数据包的功能是什么？

8. 请画图说明 DUAL 有限状态机。

9. EIGRP 除了路由表，还有哪些表格？

10. 实训操作题 1：请按照图 8-21 所示的 IPv4 网络环境配置 EIGRP，并测试配置的结果。

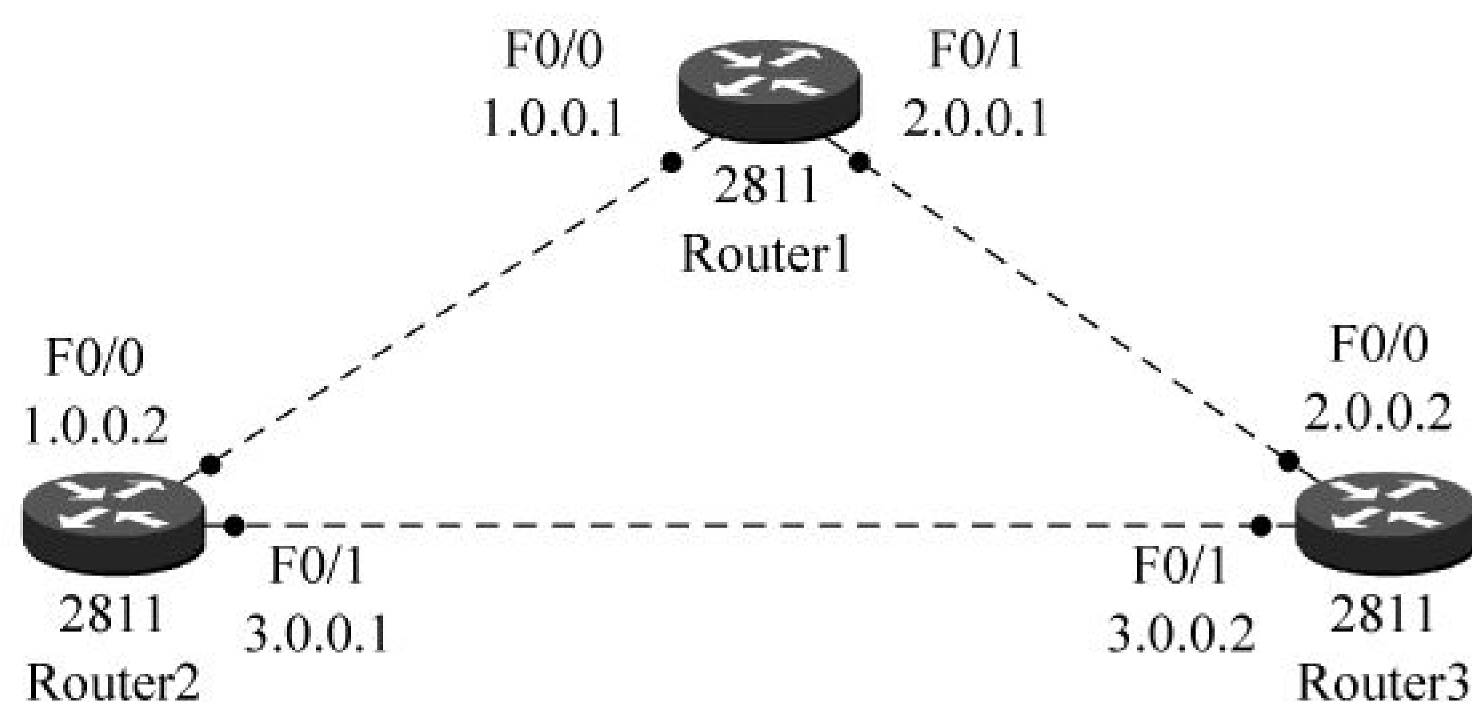


图 8-21 实训操作题 1 的网络环境

11. 实训操作题 2：请按照图 8-22 所示的 IPv6 网络环境配置 EIGRP，并测试配置的结果。

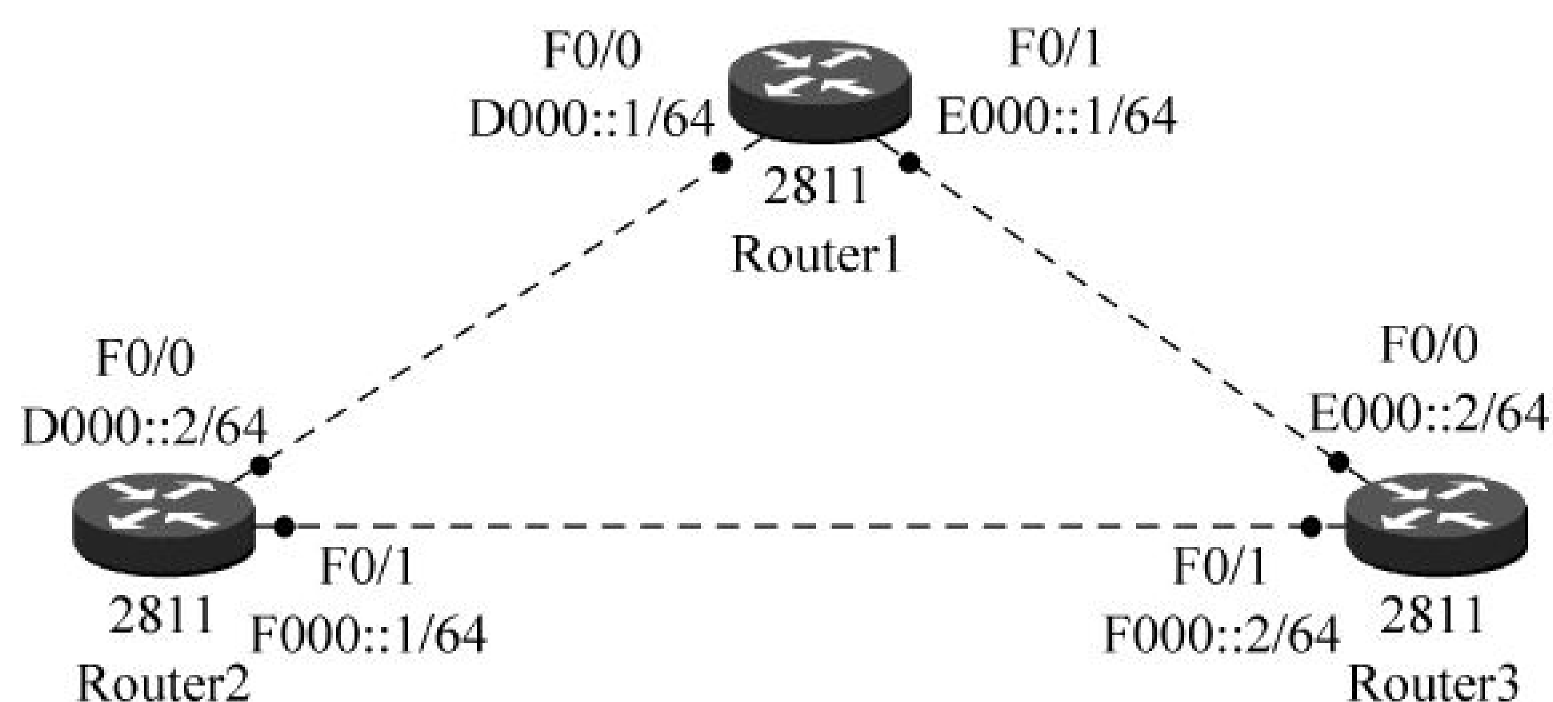


图 8-22 实训操作题 2 的网络环境

第9章 访问控制列表

CHAPTER 9

在日常工作中，网络管理员往往需要拒绝某些不允许的访问连接，同时又要允许某些正常的访问连接。例如，网络管理员希望允许局域网内的用户访问 Internet，但是又不允许局域网以外的用户通过 Internet 使用远程终端方式（Telnet）登录到局域网。通过访问控制列表（Access Control Lists，ACL）可以轻易地完成这些任务。访问控制列表是路由器自带的一种网络安全管理技术，是一个控制网络的数据流的有力工具。

访问控制列表使用包过滤手段，在路由器上分析第三层或第四层数据包头中的信息，如源地址、目的地址、源端口、目的端口以及上层协议等，并根据预先定义的规则决定哪些数据包可以转发、哪些数据包需要丢弃，从而达到访问控制的目的。

9.1 访问控制列表概述

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它是保证网络安全最重要的核心策略之一。访问控制涉及的技术也比较广，包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。

访问控制列表是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪些数据包可以转发、哪些数据包需要丢弃。至于数据包是被转发，还是被丢弃，可以根据源地址、目的地址、端口号等的特定指示条件决定。

访问控制列表不但可以起到控制网络流量、流向的作用，而且在很大程度上起到保护网络设备、服务器的关键作用。作为外网进入企业内网的第一道关卡，路由器上的访问控制列表成为保护内网安全的有效手段。

访问控制列表可以限制网络流量、提高网络性能；是提供网络安全访问的基本手段；在路由器端口处决定哪种类型的数据包被转发或被阻塞。

此外，在路由器的许多其他配置任务中都需要使用访问控制列表，如网络地址转换（Network Address Translation，NAT）、按需拨号路由（Dial on Demand Routing，DDR）、路由重分布（Routing Redistribution，RR）、策略路由（Policy-Based Routing，PBR）等很多场合都需要访问控制列表。

9.1.1 访问控制列表的功能

使用访问控制列表可以保护资源结点，阻止非法用户对资源结点访问，也可以限制特定用户结点的访问权限。例如，限制企业的人事部门使用 WWW 服务，就可以通过访问控制

列表来实现；又如，为了企业会计部门的安全，既不允许会计部门的计算机访问外网，也不允许外网访问会计部门的计算机，这一特殊要求同样可以通过访问控制列表来实现。

访问控制列表是保护网络资源的一种实用的网络安全技术。访问控制列表的主要功能可以分为两种：分类和过滤。

1. 分类

路由器使用访问控制列表来识别特定的数据流。访问控制列表识别数据流并将它们分类后，就可以通过预先配置的规则指示路由器如何处理这些数据流。例如，可以使用访问控制列表识别来自某个子网的数据流，然后在拥塞的广域网链路上授予这些数据流较高的优先级，使之优先转发。

分类可以使网络管理员能够对访问控制列表定义的数据流进行特殊处理，例如。

(1) 识别要将其从一种路由选择协议重分发到另一种路由选择协议中的路由。

(2) 识别通过虚拟专用网(VPN)连接进行传输时需要加密的数据流。

(3) 结合使用路由过滤来确定要将哪些路由包含在路由器之间传输的路由选择更新中。

(4) 结合基于策略的路由选择来确定通过专用链路传输哪些数据流。

(5) 结合服务质量(QoS)来确定发生网络拥塞时应调度队列中的哪些数据流。

(6) 结合网络地址转换(NAT)技术来确定要转发哪些数据流。

2. 过滤

默认情况下，所有数据包都被允许进入和离开所有的路由器接口。

访问控制列表通过在路由器接口处控制数据包被转发或者被丢弃，来实现对网络流量的过滤。路由器根据访问控制列表中指定的条件来检测通过路由器的每个数据包，并且决定是否丢弃数据包。在访问控制列表中指定的条件，既可以是数据包的源地址，也可以是目的地址，还可以是上层协议或者其他条件。

Cisco 提供了允许或拒绝以下数据流通过的访问控制列表：

(1) 来自或前往特定路由器接口的数据流。

(2) 来自或前往路由器的虚拟终端(VTY)接口，用于管理路由器的远程登录(Telnet)数据流。

9.1.2 建立访问控制列表的作用

具体地说，建立访问控制列表具有以下 5 个方面的作用。

1. 限制用户的行为

在路由器的接口处，决定哪种类型的数据包可以被转发，哪种类型的数据包需要丢弃。例如，禁止本企业的员工用 QQ 聊天、看股市行情、玩网络游戏等，仅靠管理手段是不够的，还必须从技术上进行控制。有两种方法可以限制网络用户的行为：第一种方法是使用访问控制列表限制用户只能使用常用的互联网服务(如仅允许浏览网页，即 80 端口)，其他服务全部过滤掉；第二种方法是封堵软件的端口或禁止用户登录特定地址的服务器。

2. 控制网络流量，提高网络性能

将访问控制列表应用到路由器接口，可以对经过接口的数据包进行检查，并根据检查的结果决定数据包是被转发，还是被丢弃，从而达到控制网络流量，提高网络性能的目的。访

问控制列表可以对通过路由器接口的数据包进行过滤，任何经过接口的数据包都要接受访问控制列表中预先定义的规则的检查，并决定数据包是转发还是丢弃，从而提高网络的性能。例如，通过访问控制列表限制用户访问 P2P 网站，以及过滤常用的 P2P 软件使用的端口，可以达到限制网络流量的目的。

3. 提高网络访问的安全级别

通过在路由器上配置访问控制列表，允许某台主机访问某个服务器，同时又阻止其他网段的主机访问相同的服务器，从而提高服务器访问的安全级别。

4. 限制网络病毒的传播

这是访问控制列表的重要作用之一。例如，蠕虫病毒在网络中传播的常用端口是TCP135、TCP139 和 TCP445，因此，使用访问控制列表过滤掉目的端口为 TCP135、TCP139 和 TCP445 的数据包，就可以阻止蠕虫病毒的传播。

5. 限制或减少路由更新的内容

访问控制列表可以限制或简化路由器选择更新的内容，常用于限制特定网络的信息通过网络传播。

9.2 访问控制列表的工作原理

访问控制列表是一组条件判断语句的集合，它定义了数据包进入路由器接口及通过路由器转发和流出路由器的行为。无论使用何种访问控制列表，其处理过程的规则都是一样的。

首先，当一个数据包进入路由器的某个接口时，路由器检查这个数据包是否可以路由或可以桥接，然后检查是否在入站接口上应用了访问控制列表。如果应用了访问控制列表，就将这个数据包与访问控制列表中的条件进行比较。如果数据包被允许通过，就继续检查路由器的其他条件，以决定是否转发到目的接口。访问控制列表并不过滤路由器本身发出的数据包，仅过滤经过路由器的数据包。

接着，路由器检查目的接口是否应用了访问控制列表，如果没有应用，就把数据包直接送到目的接口输出。

访问控制列表的执行过程如图 9-1 所示。

路由器按顺序自上而下地检查访问控制列表中的条件语句，每次将数据包与一个条件语句进行比较。找到与数据包报头匹配的语句后，将跳过其他语句，并根据匹配的语句允许或拒绝数据包。如果数据包报头与当前语句不匹配，则将其与下一跳语句进行比较。这个匹配过程将不断进行下去，直到到达访问控制列表的末尾。

最后的隐式语句与不符合任何条件的数据包匹配。这个测试条件与剩下的所有数据包匹配，并执行拒绝操作。也就是说，路由器不是把它们转发到目的接口，而是把它们丢弃。这条最后的语句通常被称为“拒绝一切数据包的隐式语句”。由于存在这条隐式语句，访问控制列表中至少应包含一条允许语句，否则将拒绝所有数据包。在路由器的配置文件中并不会显示拒绝所有数据包的隐式语句。

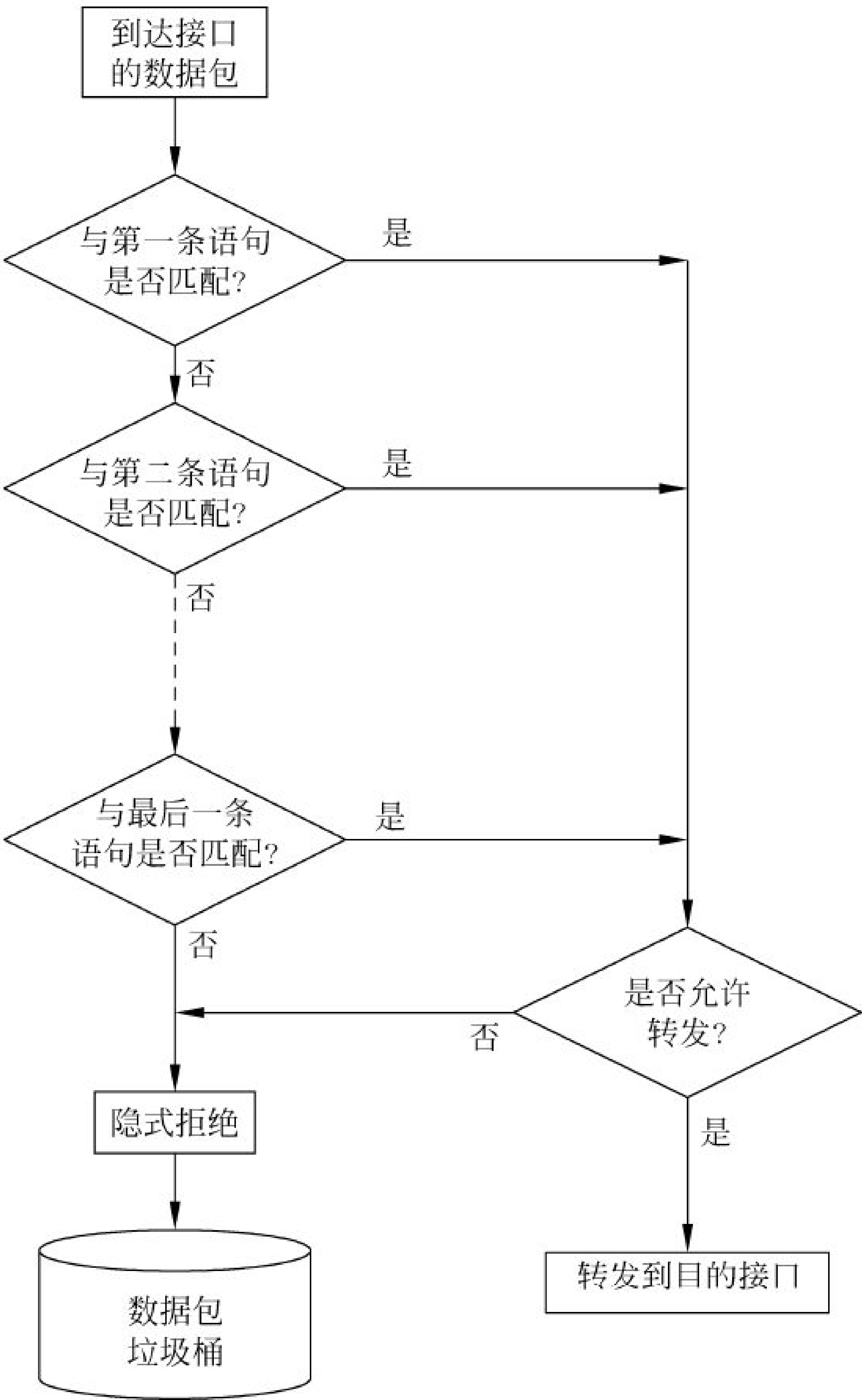


图 9-1　访问控制列表的执行过程

9.3　访问控制列表的分类和原则

9.3.1　访问控制列表的分类

目前,访问控制列表主要分为标准 ACL、扩展 ACL 和命名 ACL 3 大类。此外,还有基于时间的 ACL、IPv6 ACL 等。

标准 ACL 的功能非常简单,只检查可以被路由的数据包的源地址,从而允许或拒绝基于网络、子网或主机 IP 地址的某一协议通过路由器。而扩展 ACL 的功能非常强大,匹配的条件更详细。但是,扩展 ACL 对路由器等网络设备的性能要求更高,对网速的影响较为明显,网络管理员需要酌情使用。

1. 标准 ACL

标准 ACL 使用 1 ～ 99 以及 1300～1999 之间的正整数作为表编号。标准 ACL 可以阻止来自某一网络的所有通信流量,或者允许来自某一特定网络的所有通信流量,或者拒绝某一协议簇(如 IP)的所有通信流量。

2. 扩展 ACL

扩展 ACL 使用 100 ～ 199 以及 2000～2699 之间的正整数作为表编号。扩展 ACL 比标准 ACL 提供了更广泛的控制范围。例如,网络管理员如果希望做到"允许外来的 Web 通信流量通过,拒绝外来的 FTP 和 Telnet 等通信流量",那么,他可以使用扩展 ACL 来达到目的,标准 ACL 不能控制得这么精确。

3. 命名 ACL

命名 ACL 用名称代替列表编号来标识访问控制列表。在标准 ACL 与扩展 ACL 中都使用表编号,而在命名 ACL 中,可以使用便于记忆的若干个字母或数字组合的字符串作为表的名称来代替表的编号。使用命名 ACL 可以删除某一条特定的控制条目,这样可以让网络管理员在使用过程中方便地进行修改。

使用命名 ACL 时,要求路由器的 iOS 为 11.2 以上的版本,并且不能以同一名字命名多个 ACL,不同类型的 ACL 也不能使用相同的名字。

9.3.2　定义 ACL 时应遵循的原则

1. ACL 的列表号指出了是哪种协议的 ACL

各种协议都有自己的 ACL,而每个协议的 ACL 又分为标准 ACL 和扩展 ACL。这些 ACL 都是通过 ACL 表编号区分的。如果在使用 ACL 时用错了表编号,那么就会出错。

2. 一个 ACL 的配置基于每种协议的每个接口的每个方向

路由器一个接口上的每种协议可以配置进入方向和送出方向两个 ACL。也就是说,如果路由器上启用了两种协议栈 IP 和 IPX(那么路由器的一个接口上可以配置 IP、IPX 两种协议),每种协议进出两个方向,则共有 4 个 ACL。

3. ACL 的语句顺序决定了对数据包的控制顺序

在 ACL 中,各个条件语句的放置顺序是很重要的。当路由器决定某一数据包是被转发还是阻塞时,会按照各个条件语句在 ACL 中的顺序,并根据各语句的判断条件,对数据包进行检查,一旦找到了某一匹配条件,就结束比较过程,不再检查以后的其他条件判断语句。

4. 最有限制性的语句应放在 ACL 语句的前面

应当把最有限制性的语句放在 ACL 语句中靠前的位置或者限制性不强的语句前面,以保证位于前面的语句不会否定后面语句的作用效果;并且应把"全部允许"或者"全部拒绝"这样的语句放在末行或接近末行,可以防止出现诸如本该拒绝(放过)的数据包被放过(拒绝)的情况。

5. 保证要被拒绝的数据包尽早被拒绝

尽量将扩展 ACL 放在靠近源的位置上,保证要被拒绝的数据包尽早被拒绝,避免浪费带宽;另外,标准 ACL 应尽量靠近目的地址,由于标准 ACL 只使用源地址,如果将其靠近源,会阻止数据包流向其他端口。

6. 允许或拒绝的先后次序

当允许的语句较少时,应当先允许后拒绝;而当拒绝的语句较少时,应当先拒绝后允许。

7. 一次性删除整个标准 ACL

在标准 ACL 里，ACL 语句不能被逐条删除，只能一次性删除整个 ACL，并且新语句只能被添加到 ACL 的末行，这意味着不可能改变已有访问控制列表的功能。如果必须改变，只有先删除已存在的 ACL，然后创建一个新 ACL，将新 ACL 应用到相应的接口上。

8. 在将 ACL 应用到接口之前，一定要先建立 ACL

首先在全局模式下建立 ACL，然后再指明 ACL 是应用于接口进方向(流入数据)，还是接口出方向(流出数据)。在接口上应用一个并不存在的 ACL 是无效的。

9. 至少要有一条"允许"的语句

因为 ACL 的最后隐含一条"全部拒绝"的命令，所以在 ACL 中应当至少有一条"允许"的语句。

10. ACL 不能过滤由本路由器上发出的数据包

ACL 只能过滤穿过本路由器的数据流量，不能过滤由本路由器上发出的数据包。

11. 入站 ACL 比出站 ACL 更加高效

路由器接口收到数据包时，应用在接口 in 方向的 ACL 起作用，数据包被该 ACL 允许后，路由器才会对数据包进行路由处理；在数据包被路由选择交付到出站接口时，应用在接口 out 方向的 ACL 起作用，对接口发送出去的数据进行检查。相比之下，入站 ACL 比出站 ACL 更加高效。

9.4 配置标准访问控制列表

标准 IP 访问控制列表用于简单的访问控制、路由过滤，且仅适用于对源地址进行过滤的场合。

1. 定义标准 ACL

标准 ACL 在路由器的全局配置模式下定义，其命令的语法格式是：

```
access-list access-list-number {permit|deny} source [source-wildcard] [log]
```

标准 ACL 配置命令中每个参数的含义说明如下：

access-list-number：访问控制列表的表编号，用来指定入口属于哪一个访问控制列表。对于标准 ACL 来说，是一个 1～99 或 1300～1999 之间的正整数。

permit：如果满足测试条件，则允许从该入口来的数据包通过。

deny：如果满足测试条件，则拒绝从该入口来的数据包通过。

source：数据包的源地址，可以是网络地址或者主机 IP 地址。

source-wildcard：这是一个可选项，称为通配符掩码，又称为反掩码，和源地址一起决定哪些位需要匹配。

log：这是一个可选项，用于生成相应的日志消息，记录经过 ACL 入口的数据包。

地址过滤是根据 ACL 的通配符掩码来实现的。通配符掩码是一个 32 位的数字字符串，它被用实心圆点分成 4 个 8 位组，并表示成点分十进制的形式。默认的通配符掩码是 0.0.0.0。在通配符掩码中，0 表示"要检查相应的位"，而 1 表示"不检查相应的位"。例如，源地址和通配符掩码分别是 172.12.10.31 和 0.0.0.255，则表明源地址的前 3 个 8 位组必

须精确匹配，而最后一个 8 位组的取值则不限，可以取任意值。

通配符掩码还有两个特殊的关键字，即 any 和 host。

通配符 any 表示所有主机，是通配符掩码 255.255.255.255 的简写形式。例如，允许所有 IP 地址的数据包通过，可以使用以下两条语句之一：

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
Router(config)#access-list 1 permit any
```

而通配符 host 表示一台主机，是通配符掩码 0.0.0.0 的简写形式。例如，只允许来自 IP 地址为 172.12.20.69 的数据包，可以使用以下两条语句之一：

```
Router(config)#access-list 1 permit 172.12.20.69 0.0.0.0
Router(config)#access-list 1 permit host 172.12.20.69
```

2. 删除一个标准 ACL

可以通过在 access-list 命令前加上 no 来删除一个已经建立的标准 ACL，其使用语法格式如下：

```
no access-list access-list-number
```

例如，如果想删除一个编号为 2 的标准访问控制列表，可以使用以下命令：

```
no access-list 2
```

如果想修改某个标准访问控制列表，则只能先用 no access-list access-list-number 命令删除这个访问控制列表，然后再重新建立新的访问控制列表。

3. 将标准 ACL 应用到某个接口上

当创建了一个标准 ACL 并且分配好表号之后，为了让这个 ACL 真正起作用，必须将它应用到一个接口上。用 access-group 命令可以实现此功能。access-group 命令的语法格式如下：

```
ip access-group access-list-number {in|out}
```

其中，参数 in 和 out 表示 ACL 作用在接口上的方向，这两个参数都是以路由器作为参照物的。如果 in 和 out 这两个参数都没有指定，则默认为 out。

4. 标准 ACL 应用示例

下面以图 9-2 所示的某企业的内部网络为例，来说明标准 ACL 的配置和验证过程。

在图 9-2 中，假设这个企业的网络通过路由器 Router1 和 Router2 互连，配置 RIPv2 路由协议，以保证网络正常通信。要求在 Router2 上配置标准 ACL，允许市场部的 IP 地址为 172.16.10.2 的主机 PC2 访问路由器 Router2，但拒绝市场部的其他主机访问路由器 Router2，并允许网络中人事部和财务部的所有其他主机访问路由器 Router2。

首先，在路由器 Router1 的全局配置模式上配置 RIPv2 路由协议，如图 9-3 所示。

接着，在路由器 Router2 的全局配置模式上配置 RIPv2 路由协议，如图 9-4 所示。

此时，可以用 show ip route 命令查看路由器 Router2 的路由表，结果如图 9-5 所示。

这时，可以从市场部的 IP 地址为 172.16.10.2 和 172.16.10.3 的两台主机的 DOS 状态下，分别用 ping 命令测试与路由器 Router2 的 IP 地址为 11.1.1.2 的接口的连通性，结果分别如图 9-6 和图 9-7 所示。

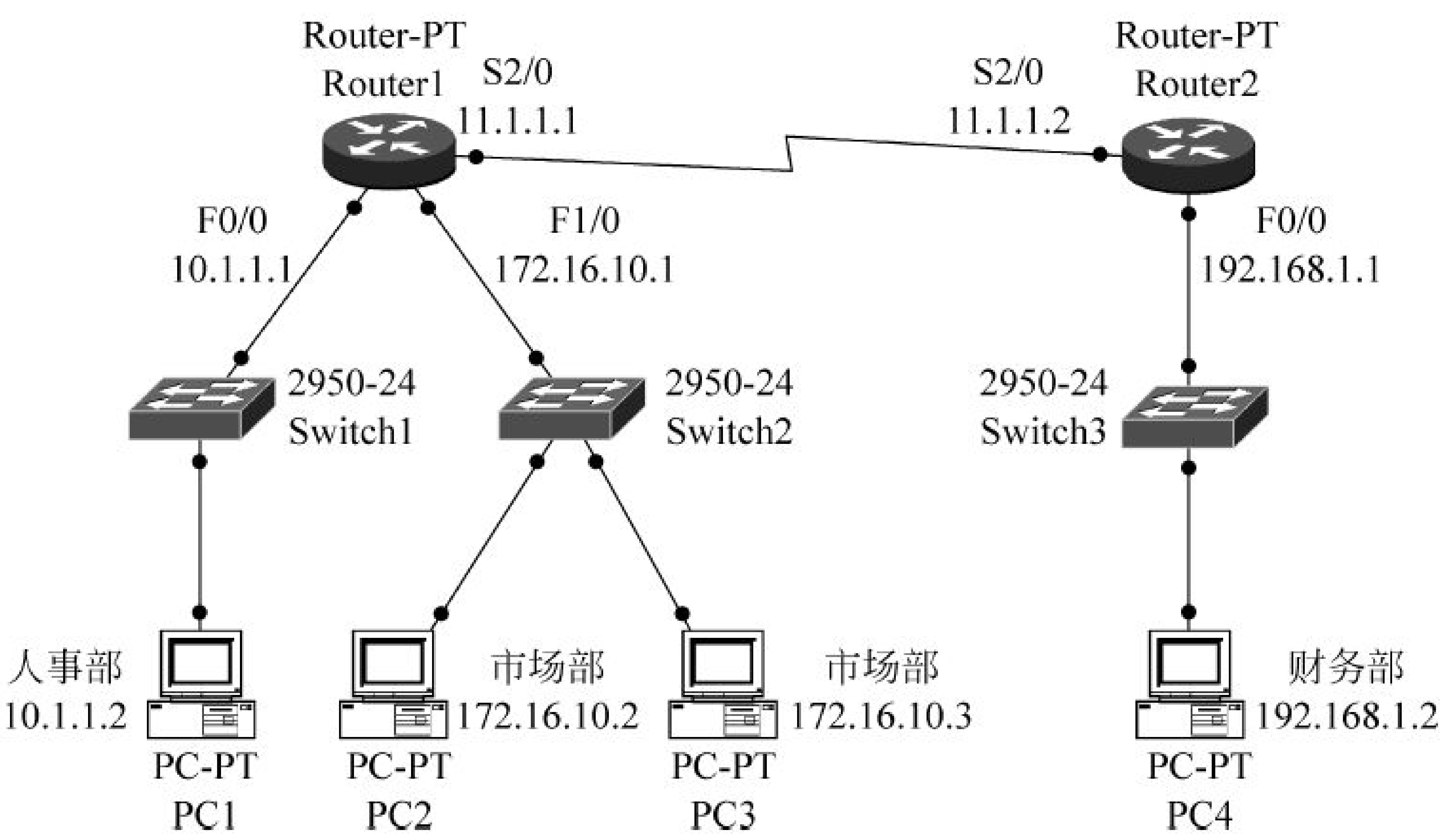


图 9-2 某企业的内部网络环境

```
Router1(config)#route rip
Router1(config-router)#version 2
Router1(config-router)#network 10.1.1.0
Router1(config-router)#network 11.1.1.0
Router1(config-router)#network 172.16.10.0
Router1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
Router1#
```

图 9-3 路由器 Router1 的 RIPv2 配置

```
Router2(config)#route rip
Router2(config-router)#version 2
Router2(config-router)#network 11.1.1.0
Router2(config-router)#network 192.168.1.0
Router2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
Router2#
```

图 9-4 路由器 Router2 的 RIPv2 配置

```
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobi
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF ir
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA externa
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
       * - candidate default, U - per-user static route, o -
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/1] via 11.1.1.1, 00:00:19, Serial2/0
C    11.0.0.0/8 is directly connected, Serial2/0
R    172.16.0.0/16 [120/1] via 11.1.1.1, 00:00:19, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
Router2#
```

图 9-5 路由器 Router2 的路由表

```
PC>ping 11.1.1.2

Pinging 11.1.1.2 with 32 bytes of data:

Reply from 11.1.1.2: bytes=32 time=63ms TTL=254
Reply from 11.1.1.2: bytes=32 time=47ms TTL=254
Reply from 11.1.1.2: bytes=32 time=47ms TTL=254
Reply from 11.1.1.2: bytes=32 time=47ms TTL=254

Ping statistics for 11.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 63ms, Average = 51ms

PC>
```

图 9-6 测试主机 172.16.10.2 与路由器 Router2 的连通性

```
PC>ping 11.1.1.2

Pinging 11.1.1.2 with 32 bytes of data:

Reply from 11.1.1.2: bytes=32 time=47ms TTL=254
Reply from 11.1.1.2: bytes=32 time=46ms TTL=254
Reply from 11.1.1.2: bytes=32 time=47ms TTL=254
Reply from 11.1.1.2: bytes=32 time=39ms TTL=254

Ping statistics for 11.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 47ms, Average = 44ms

PC>
```

图 9-7 测试主机 172.16.10.3 与路由器 Router2 的连通性

图 9-6 和图 9-7 表明当前市场部的这两台主机与路由器 Router2 都是正常连通的。

下面在 Router2 上按前面指定的要求配置标准 ACL，即允许市场部的 IP 地址为 172.16.10.2 的主机 PC2 访问路由器 Router2，但拒绝市场部的其他主机访问路由器 Router2，并允许网络中的其他所有主机访问路由器 Router2。具体的配置命令如图 9-8 所示。

```
Router2(config)#access-list 1 permit host 172.16.10.2
Router2(config)#access-list 1 deny 172.16.10.2 0.0.0.255
Router2(config)#access-list 1 permit any
Router2(config)#interface s2/0
Router2(config-if)#ip access-group 1 in
```

图 9-8 在路由器 Router2 上配置标准 ACL

然后，可以用 show access-lists 命令验证配置好的访问控制列表，结果如图 9-9 所示。

```
Router2#show access-lists
Standard IP access list 1
    permit host 172.16.10.2 (4 match(es))
    deny 172.16.10.0 0.0.0.255 (4 match(es))
    permit any (24 match(es))
Router2#
```

图 9-9 查看路由器 Router2 的访问控制列表

接着，可以用 show ip interface 命令查看 ACL 作用在接口上的信息，并查看 ACL 是否正确配置，结果如图 9-10 所示。

此时，从市场部的 IP 地址为 172.16.10.2 的主机 ping 路由器 Router2 的 IP 地址为 11.1.1.2 的接口，结果如图 9-11 所示，表明两者能够连通；再从市场部的 IP 地址为 172.16.10.3 的主机 ping 路由器 Router2 的 IP 地址为 11.1.1.2 的接口，结果如图 9-12 所示，表明两者不能连通。

```
Serial2/0 is up, line protocol is up (connected)
  Internet address is 11.1.1.2/8
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  ……
```

图 9-10　查看 ACL 作用在接口上的信息

```
PC>ping 11.1.1.2

Pinging 11.1.1.2 with 32 bytes of data:

Reply from 11.1.1.2: bytes=32 time=78ms TTL=254
Reply from 11.1.1.2: bytes=32 time=36ms TTL=254
Reply from 11.1.1.2: bytes=32 time=45ms TTL=254
Reply from 11.1.1.2: bytes=32 time=39ms TTL=254

Ping statistics for 11.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 78ms, Average = 49ms

PC>
```

图 9-11　再次测试主机 172.16.10.2 与路由器 Router2 的连通性

```
PC>ping 11.1.1.2

Pinging 11.1.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 11.1.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

图 9-12　再次测试主机 172.16.10.3 与路由器 Router2 的连通性

同样，也可以用 ping 命令测试人事部 IP 地址为 10.1.1.2 的主机与路由器 Router2 的 IP 地址为 11.1.1.2 的接口的连通性，结果如图 9-13 所示，表明两者的连通正常。

```
PC>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=8ms TTL=128
Reply from 10.1.1.2: bytes=32 time=8ms TTL=128
Reply from 10.1.1.2: bytes=32 time=5ms TTL=128
Reply from 10.1.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 6ms

PC>
```

图 9-13　测试主机 10.1.1.2 与路由器 Router2 的连通性

9.5　用标准 ACL 限制虚拟终端的访问

一般来说，路由器上的物理接口都是虚拟终端接口，即 VTY 接口，路由器上共有 5 个 VTY 接口，它们的编号为 0～4。基于安全上的考虑，网络管理员可以允许或禁止用户通过 VTY 方式访问路由器，也可以拒绝从路由器上访问某个目的地址的主机。例如，网络管理员可以配置 ACL，允许通过远程终端方式访问路由器，以达到远程管理路由器的目的。

限制 VTY 的访问不是简单的数据包转发控制机制，而是用作提高网络的安全性。VTY 使用 Telnet 协议对路由器进行远程访问，与路由器产生一个非物理性的连接。这种限制应配置在所有的 VTY 连接中，因为它不能控制用户使用哪个连接登录路由器。

VTY ACL 的创建与在接口上建立 ACL 是一样的，但是在应用 VTY ACL 到虚拟连接时，要用命令 access-class 代替命令 access-group。

下面以图 9-14 为例，说明如何通过标准 ACL 限制虚拟终端的访问，只允许 IP 地址为 10.0.0.101 的主机远程登录路由器 Router1，并拒绝其他所有主机远程登录路由器 Router1。

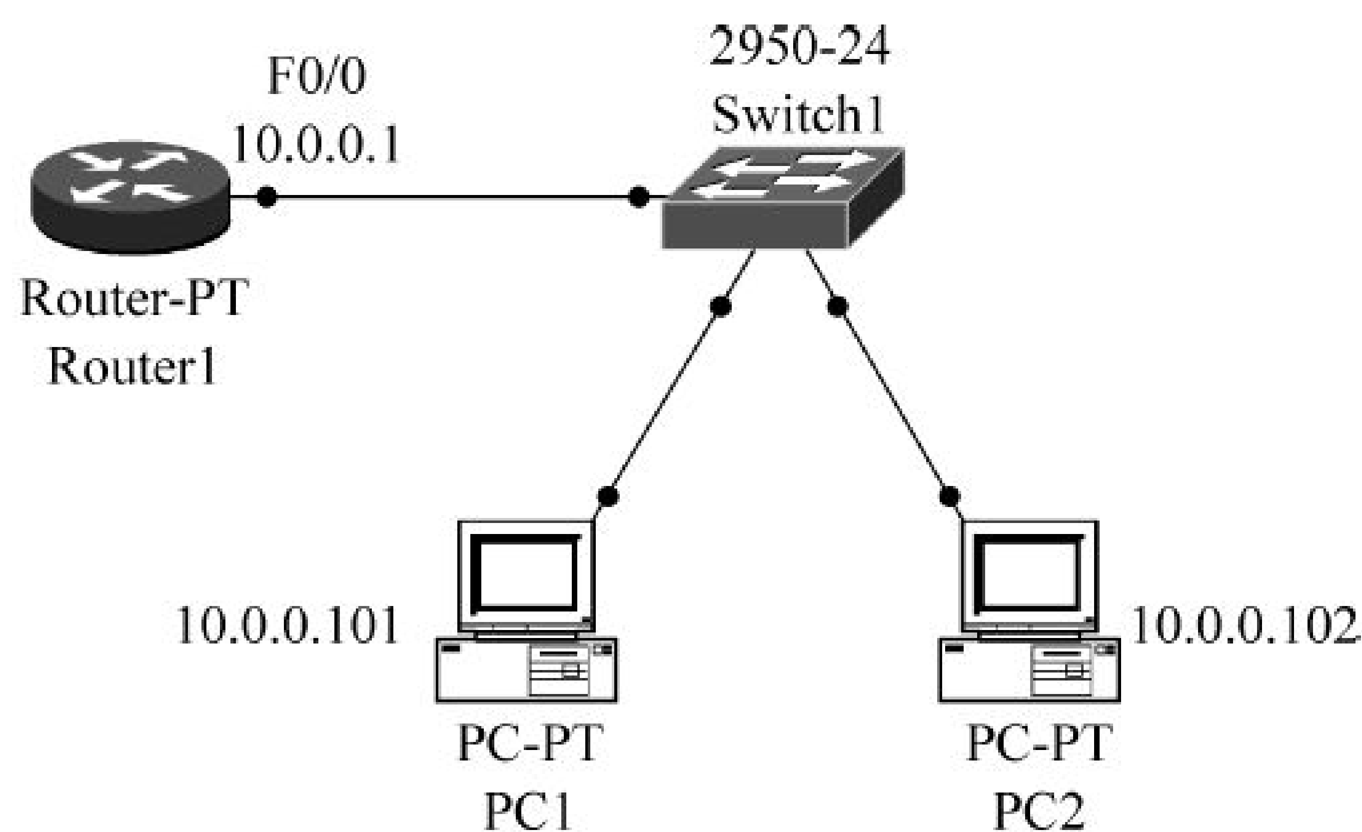


图 9-14　限制 Telnet 访问的网络环境

配置 VTY 连接的访问控制列表时，首先要注意以下几点：

(1) 在配置接口的访问控制列表时，可以使用数字编号 ACL，也可以使用命名 ACL。

(2) 但是，只有使用数字编号的访问控制列表才可以应用到 VTY 中。

(3) 用户可以连接所有的 VTY，因此所有的 VTY 连接都要应用相同的 ACL。

在图 9-14 所示的网络环境中，可以在路由器 Router1 的全局配置模式下使用如图 9-15 所示的命令配置 VTY 连接的 ACL。

```
Router1(config)#access-list 1 permit host 10.0.0.101
Router1(config)#line vty 0 4
Router1(config-line)#password supervisor
Router1(config-line)#login
Router1(config-line)#access-class 1 in
Router1(config-line)#
```

图 9-15　用标准 ACL 限制 Telnet 访问

配置 ACL 完成后，可以从 10.0.0.101 主机 Telnet 访问路由器，结果如图 9-16 所示，表明此时可以用 Telnet 方式远程登录。

此时如果从 10.0.0.102 主机 Telnet 访问路由器，结果如图 9-17 所示，表明拒绝用 Telnet 方式远程登录。

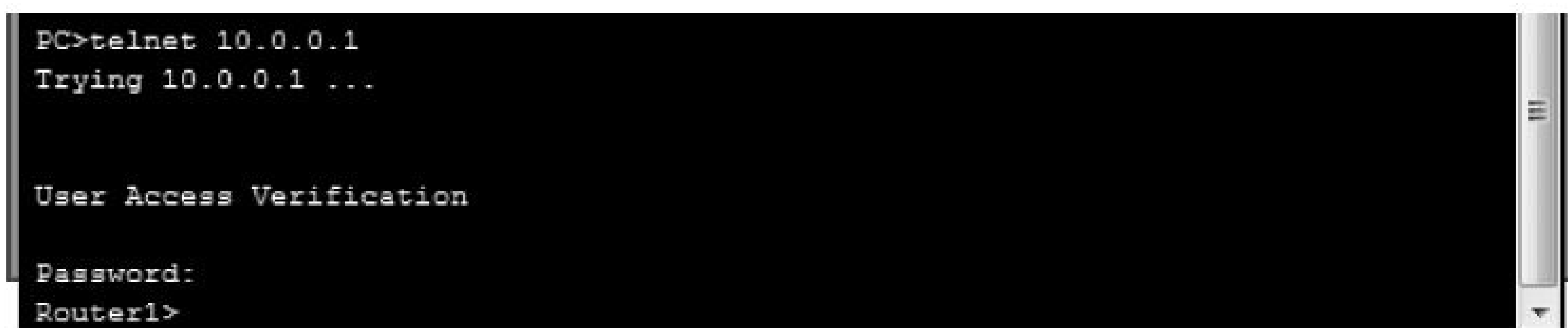


图 9-16　从 10.0.0.101 主机 Telnet 访问路由器



图 9-17　从 10.0.0.102 主机 Telnet 访问路由器

9.6　配置扩展访问控制列表

标准 ACL 只能根据源地址来检查数据包，它允许/拒绝的整个 TCP/IP 协议集的数据功能有限。而扩展的访问控制列表功能强大，它可以控制源 IP、目的 IP、源端口、目的端口等，能将控制条件细化，配置更加灵活。但是，扩展 ACL 也存在一个缺点，就是对网络设备性能、网络带宽的要求更高，组网时需要酌情使用。

1. 定义扩展 ACL

定义扩展 ACL 仍然使用 access-list 命令，在全局配置模式下使用，其命令格式如下：

```
access - list access - list - number {permit | deny} protocol source [source - wildcard]
destination [destination - wildcard] [operator operand] [established] [log]
```

其中，每个参数的详细说明如下：

access-list-number(表编号)：扩展 ACL 使用一个 100～199 或 2000～2699 的正整数来标识。

策略：可以选择 permit(允许)或 deny(拒绝)。

protocol(协议)：检查特定协议的数据包，如 TCP、UDP、ICMP、IP 等协议。

source [source-wildcard](源地址及通配符掩码)：指定 IP 网段时，用“IP 地址＋通配符掩码”表示；指定单个主机地址时，用“host＋IP 地址”表示；任意地址则用“any”表示。通配符掩码为可选项，可以省略不写。

destination [destination-wildcard](目的地址及通配符掩码)：指定 IP 网段：IP 地址＋通配符掩码；单个主机地址：host；任意地址：any。通配符掩码为可选项，可以省略不写。

operator(目的端口)：此项为可选项，可以省略不写，可用的操作符包括 lt(小于)、gt(大于)、eq(等于)、neq(不等于)和 range(包括的范围)。如果操作符位于源地址和源地址通配符之后，那么它必须匹配源端口。如果操作符位于目的地址和通配符之后，那么它必须匹配目的端口。range 操作符需要两个端口号，其他操作符只需要一个端口号。

operand(端口号)：此项为可选项，指明 TCP 或 UDP 端口的十进制数字或名字。端口可以为 0～65 535。

established：这个选项用于 TCP，指示已建立的连接。

TCP 数据包的报头中有 6 个控制位，分别是 URG、ACK、PSH、RST、SYN、FIN。在整个 TCP 数据传输过程中，ACK 位除了在第一次握手的时候为 0 外，其他任何时候都是置 1 的，根据这个原理可以控制 TCP 连接的方向。当路由器收到一个数据包并匹配到带有 established 的 ACL 时，established 会检查 ACK 和 RST 位，如果两个控制位都没被设置(使用)，就表明源地址正在向目标地址建立 TCP 连接，这与 established 选项的含义不一致，数据包将被拒绝通过，也就是拒绝该源地址发起建立 TCP 连接的请求。established 只对 TCP 连接起作用，对 UDP 不起作用。

log：这是一个可选项，用于生成相应的日志消息，记录经过 ACL 入口的数据包。

2. 常用的 TCP 和 UDP 端口号

表 9-1 中列出了常用的 TCP 和 UDP 端口号。

表 9-1 常用的 TCP 和 UDP 端口号

端 口 号	协 议	关 键 字	说 明
7	TCP、UDP	ECHO	回声
20	TCP、UDP	FTP-DATA	文件传输协议(数据)
21	TCP、UDP	FTP	文件传输协议(控制)
23	TCP、UDP	TELNET	远程虚拟终端登录
25	TCP、UDP	SMTP	简单邮件传输协议
53	TCP、UDP	DOMAIN	域名服务器(DNS)
67	UDP	DHCP	动态主机配置协议
69	UDP	TFTP	简单文件传输协议
80	TCP	HTTP	超文本传输协议(WWW)
110	TCP	POP3	第 3 版邮件接收协议
161	TCP、UDP	SNMP	简单网络管理协议

3. 将扩展 ACL 应用到某个接口

与标准 ACL 相似，扩展 ACL 也要用 ip access-group 命令把一个已经建立好的扩展 ACL 应用到某个接口。命令格式如下：

```
ip access - group access - number {in|out}
```

这里，ip access-group 命令带有两个参数：表号和方向。

(1) access-number(表号)：与该接口关联的访问控制列表表号。

(2) 方向有两个选项，即 in 或 out，in 表示对所有入站的数据进行匹配，out 表示对所有出站的数据进行匹配。

4. 扩展 ACL 应用示例

下面以图 9-18 所示的某企业的网络环境为例，说明扩展 ACL 的配置和验证过程。

在图 9-18 所示的网络环境中，假设有网络中心和市场部两个部门，通过两个路由器 Router1 和 Router2 相连。要求在路由器 Router1 上配置扩展 ACL，实现以下 5 个功能：

(1) 允许市场部子网 10.0.0.0 的所有主机访问网络中心的 Web 服务器 192.168.1.2 (注：Web 服务器使用 TCP，80 号端口)。

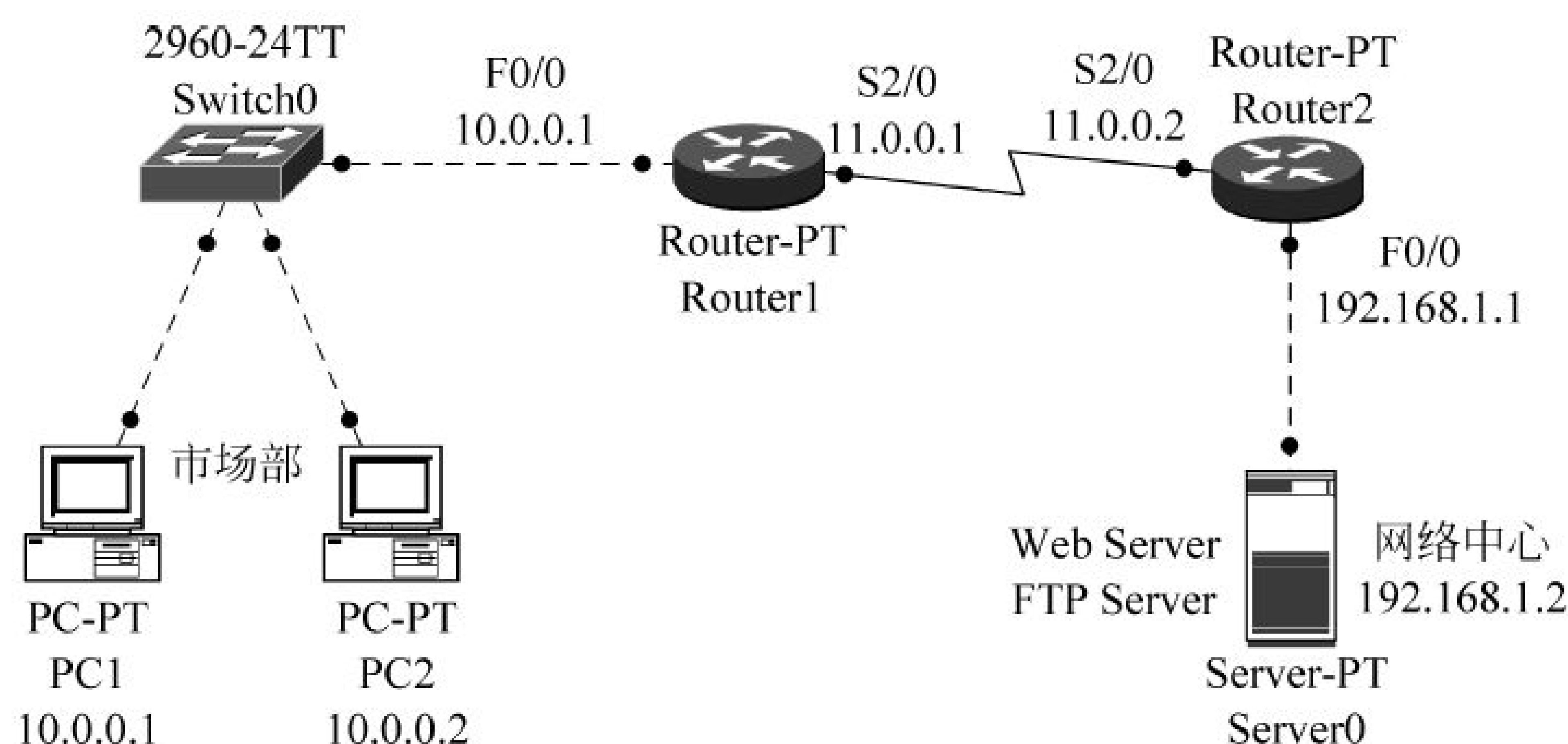


图 9-18 扩展 ACL 的配置环境

(2) 拒绝市场部 10.0.0.2 的主机访问网络中心的 FTP 服务器 192.168.1.2(注：FTP 服务器使用 TCP,使用 20 号端口传输数据,21 号端口传输控制命令)。

(3) 拒绝市场部子网 10.0.0.0 的所有主机远程登录(即 Telnet 方式)路由器 Router2(注：Telnet 协议使用 TCP,23 号端口)。

(4) 拒绝市场部 10.0.0.2 的主机 ping 路由器 Router2 的 11.0.0.2 接口(注：ping 命令使用 ICMP)。

(5) 拒绝市场部 10.0.0.2 的主机 ping IP 地址为 192.168.1.2 的服务器(ICMP)。

在路由器 Router1 的全局配置模式下配置扩展 ACL,如图 9-19 所示。

```
Router1(config)#access-list 100 permit tcp 10.0.0.0 0.0.0.255 host 192.168.1.2
eq 80
Router1(config)#access-list 100 deny tcp 10.0.0.0 0.0.0.255 host 192.168.1.2 eq
20
Router1(config)#access-list 100 deny tcp 10.0.0.0 0.0.0.255 host 192.168.1.2 eq
21
Router1(config)#access-list 100 deny tcp 10.0.0.0 0.0.0.255 host 11.0.0.2 eq 23
Router1(config)#access-list 100 deny icmp host 10.0.0.2 host 11.0.0.2
Router1(config)#access-list 100 deny icmp host 10.0.0.2 host 192.168.1.2
Router1(config)#access-list 100 permit ip any any
Router1(config)#interface f0/0
Router1(config-if)#ip access-group 100 in
Router1(config-if)#
```

图 9-19 配置扩展 ACL 实例

验证扩展 ACL 的方法与验证标准 ACL 的方法相似,都可以使用 show access-list、show ip interface 和 ping 等命令,这里就不再赘述了。

9.7 配置命名的访问控制列表

不管是标准 ACL,还是扩展 ACL,仅用编号区分 ACL 不便于网络管理员识别 ACL。所以,Cisco 公司从 iOS 11.2 版开始引入了命名 ACL。

9.7.1 命名 ACL 与编号 ACL 的区别

命名 ACL 与编号 ACL 的工作原理相同,两者的主要区别如下：

(1) Cisco iOS 软件 11.2 之前的版本不支持命名 ACL。

(2) 名字能直观地反映出 ACL 完成的功能。

(3) 命名 ACL 没有数量的限制。

(4) 当修改 ACL 时,编号 ACL 只能删除整个 ACL 后重新定义,而命名 ACL 允许删除任意指定的语句,但是命名 ACL 新增加的语句只能放到 ACL 后。

(5) 同一个路由器上的命名 ACL 的名称在所有协议和类型中都必须是唯一的,而不同路由器上的命名 ACL 名称可以相同。

(6) 命名 ACL 是一个全局命令,它使路由器进入到命名 ACL 的配置模式,在该模式下可以建立匹配和允许/拒绝动作的相关语句。

9.7.2 配置命名 ACL 的语法格式

1. 定义命名 ACL

定义命名 ACL 使用 ip access-list 命令,其语法格式如下:

```
ip access - list {standard|extended} name
```

这个命令使路由器进入 ACL 配置模式。ACL 配置模式的提示符是在路由器名称后紧接(config-std-nacl)或(config-ext-nacl)。第 1 个参数代表 ACL 的类型,而第 2 个参数则是命名 ACL 的名称,用于取代原来的表编号。当第 1 个参数为 standard 时,用于定义标准命名 ACL;当第 1 个参数为 extended 时,用于定义扩展命名 ACL。

命名的 ACL 可以用于标准 ACL 和扩展 ACL 中,命名 ACL 的名称必须以字母开头,并且要区分大小写字母。在名称的中间可以包含任何字母和数字混合使用的字符,也可以在其中包含方括号"[ ]"、大括号"{ }"、下画线"_"、减号"-"、加号"+"、除号"/"以及"\"
"&""#""@"和"!"等特殊字符。ACL 名称的最大长度为 100 个字符。

2. 指定允许或拒绝的条件

在 ACL 配置模式下可以指定一个或多个允许或拒绝的条件,来决定数据包是被转发,还是被丢弃,语法格式如下:

```
permit {source [source - wildcard]|any}
```

或

```
deny {source [source - wildcard]|any}
```

其中,操作符 permit 表示允许,而命令 deny 表示拒绝。

参数 source [source-wildcard]表示源地址和通配符掩码。指定 IP 网段时,用"IP 地址+通配符掩码"表示;指定单个主机地址用"host+IP 地址"表示;任意地址则用 any 表示。通配符掩码为可选项,可以省略。

3. 将命名 ACL 应用到某个接口

与标准 ACL 和扩展 ACL 相似,命名 ACL 也要用 ip access-group name 命令把一个已经建立好的扩展 ACL 应用到某个接口。命令格式如下:

```
ip access - group name {in|out}
```

同样,ip access-group 命令带有两个参数,name 是表名,必须与前面定义命名 ACL 时

的表示一致；而 in 或 out 表示方向。

4. 配置标准命名 ACL 示例

下面以图 9-20 所示的网络环境为例，说明标准命名 ACL 的配置方法。

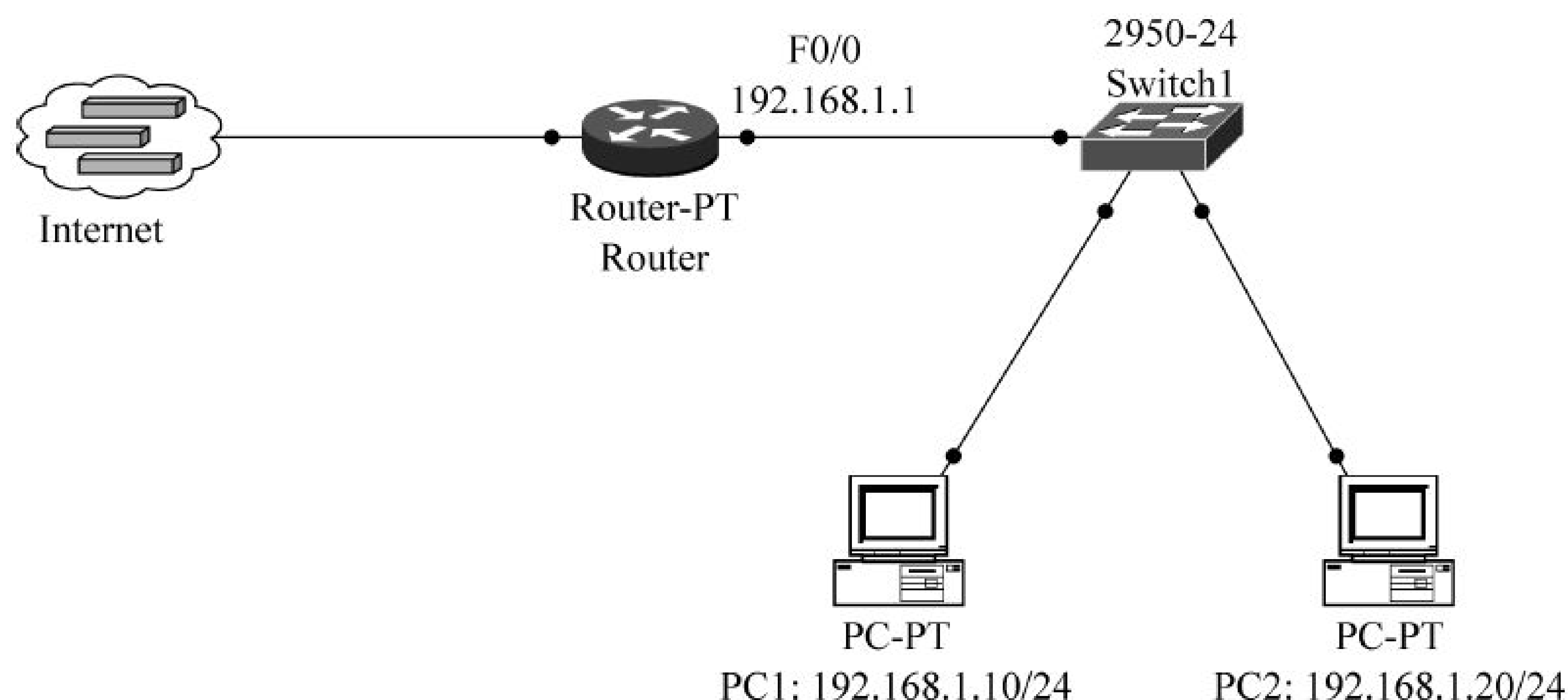


图 9-20 标准命名 ACL 的网络环境

要求在路由器 Router 上进行配置，拒绝来自某部门子网 192.168.1.0/24 的数据包，并允许转发所有其他部门的数据包。配置命令如图 9-21 所示。

```
Router(config)#ip access-list standard acl_std
Router(config-std-nacl)#deny 192.168.1.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface f0/0
Router(config-if)#ip access-group acl_std in
Router(config-if)#
```

图 9-21 配置标准命令 ACL 实例

5. 配置扩展命名 ACL 示例

这里，仍然以图 9-20 所示的网络环境为例，说明扩展命名 ACL 的配置方法。假设仅拒绝来自这个部门子网中的 FTP(注：FTP 使用 TCP 的端口号 20 和 21)和 Telnet 数据包(注：Telnet 使用 TCP 的端口号 23)，而允许转发所有其他部门的数据包。配置命令如图 9-22 所示。

```
Router(config)#ip access-list extended acl_ext
Router(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 any eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 any eq 21
Router(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 any eq 23
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface f0/0
Router(config-if)#ip access-group acl_ext in
Router(config-if)#
```

图 9-22 配置扩展命令 ACL 实例

9.8 配置基于时间的访问控制列表

基于时间的 ACL 可以在不同的时间段实施访问控制。在原有 ACL 的基础上应用时间段。时间段可以分为 3 种：绝对(absolute)时间段、周期(periodic)时间段和混合时间段。

1. 设置路由器系统时间

为了在不同的时间段实施访问控制，首先需要设置路由器系统时间。其语法格式如下：

```
R1#clock set 时:分:秒 日 月 年
```

例如：R1#clock set 14:08:37 21 may 2018

说明：在配置基于时间的 ACL 之前，要确保路由器系统时间设置正确。

2. 定义时间段名称

定义时间段名称使用 time-range 命令，该命令除了定义时间段的名称外，还使路由器进入时间段配置模式，提示符变为(config-time-range)。其语法格式如下：

```
R1(config)#time-range 名称
```

其中，名称可以取字符、数字或者字符+数字。

例如：

```
R1(config)#time-range t1                    //定时时间段,名称为 t1
R1(config-time-range)#                      //进入时间段配置模式
```

3. 定义绝对时间段

定义绝对时间段使用 absolute start 命令，为时间范围指定一个绝对的开始和结束时间。其语法格式如下：

```
R1(config-tmie-range)#absolute start 开始时间 end 结束时间
```

其中，开始时间的格式是时:分日月年

而结束时间的格式同样是时:分日月年

例如：

```
R1(config-time-range)#absolute start 8:00 21 may 2018 end 18:00 21 may 2018
```

4. 定义周期时间段

周期时间段的周期是指一个星期。定义周期时间段的语法格式如下：

```
R1(config-time-range)#periodic 开始时间 to 结束时间
```

其中，开始时间或结束时间可以是一个星期中的某一天或某几天。星期一至星期日依次用相应的英文单词表示，即 Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、Sunday；从星期一(Monday)到星期五(Friday)，即工作日，用 Weekday 表示；星期一至星期日，即每天用 Daily 表示；而星期六到星期日(周末)则用 Weekend 表示。

例如：

```
R1(config-time-range)#periodic weekend 8:00 to 18:00     //星期六和星期日 8:00 到 18:00
```

```
R1(config-time-range)#periodic daily 8:00 to 18:00        //一周中每天 8:00 到 18:00
R1(config-time-range)#periodic wednesday 15:00 to saturday 8:00
                                                          //星期三 15:00 到星期六 8:00
```

说明：每个时间段只能有一个 absolute 语句，但可以有多个 periodic 语句。

5. 调用已经定义的时间段

时间段定义之后，可以在访问控制列表中用 time-range 调用已经定义的时间段；

例如：

```
access-list 100 permit tcp any any eq 80 time-range t1
```

说明：在调用时间段时，只有配置了相应的 time-range 的时间段规则，才能在指定的时间段内生效。

6. 查看时间段

可以使用命令 show time-range 查看已经定义的时间段，也可以用命令“show access-list 表名”查看与指定的访问控制列表关联的时间段。

9.9 配置 IPv6 访问控制列表

像 IPv4 一样，在 IPv6 路由器上也可以定义和启用标准的和扩展的 IPv6 ACL 来控制 IPv6 流量。

9.9.1 创建 IPv6 访问控制列表

创建 IPv6 ACL 的命令是 ipv6 access-list，其作用是给每个 ACL 定义一个唯一的表名。命令的语法格式如下：

```
ipv6 access-list 表名
```

例如：

```
Router(config)#ipv6 access-list acllist1
```

以上命令的作用是建立一个表名为 acllist1 的访问控制列表。

在定义 ACL 之后，系统进入 ipv6 acl 配置子模式，提示符为(config-ipv6-acl)。

9.9.2 在接口上应用 IPv6 访问控制列表

在定义 ACL 之后，最后的步骤是将这个 ACL 应用到路由器的某个接口。其相应的命令与 IPv4 的命令并不一样，在 IPv6 中将一个 IPv6 ACL 应用到接口的命令是 ipv6 traffic-filter。这个命令的语法格式如下：

```
Router(config)#ipv6 traffic-filter access-list-name {in|out}
```

9.9.3 配置标准 IPv6 访问控制列表

与 IPv4 一样，IPv6 ACL 的策略由一条和几条使用 permit(允许)或 deny(拒绝)的命令

组成。每条 ACL 命令必须至少定义协议类型、要匹配的源地址或目的地址。在 IPv6 中，如果所有的 ACL 命令都不匹配，则最后会自动应用隐含命令 deny ipv6 any any。在 IPv6 中，any 地址的意思与::/0 等价。

1. 定义标准 IPv6 ACL

定义标准 IPv6 ACL 使用 ipv6 access-list 命令。其语法格式如下：

```
ipv6 access - list access - list - name
```

其中，access-list-name 是定义的标准 ACL 的表名。

2. 指定允许或拒绝数据包的条件

指定允许或拒绝数据包的条件使用以下命令：

```
permit | deny {source - ipv6 - prefix/prefix - length | any | host host - ipv6 - address}
{destination - ipv6 - prefix/prefix - length | any | host host - ipv6 - address}
[log | log - input]
```

其中每个参数的含义说明如下：

permit：如果满足测试条件，则允许数据包通过该接口。

deny：如果满足测试条件，则拒绝数据包通过该接口。

source-ipv6-prefix/prefix-length：源 IPv6 地址的前缀及前缀的长度，数据包从这个源地址出发。

any：表示任意 IPv6 地址，与::/0 等价。

host：一个单独的 IPv6 地址，这个关键字只能在配置子模式中使用。

destination：目的 IPv6 前缀和前缀的长度，数据包的目的地。

log：这是一个可选项，用于生成 IPv6 日志，记录经过接口的数据包。

log-input：IPv6 访问列表日志记录的 log 关键字。使用这个关键字，只要可行，日志将会记录输入接口和源 MAC 地址。

3. 删除一个 IPv6 ACL

要删除一个 IPv6 ACL，使用“no ipv6 access-list 表名”命令即可。

4. 配置标准 IPv6 ACL 实例

下面以图 9-23 所示的网络环境为例，说明配置标准 IPv6 ACL 的方法。

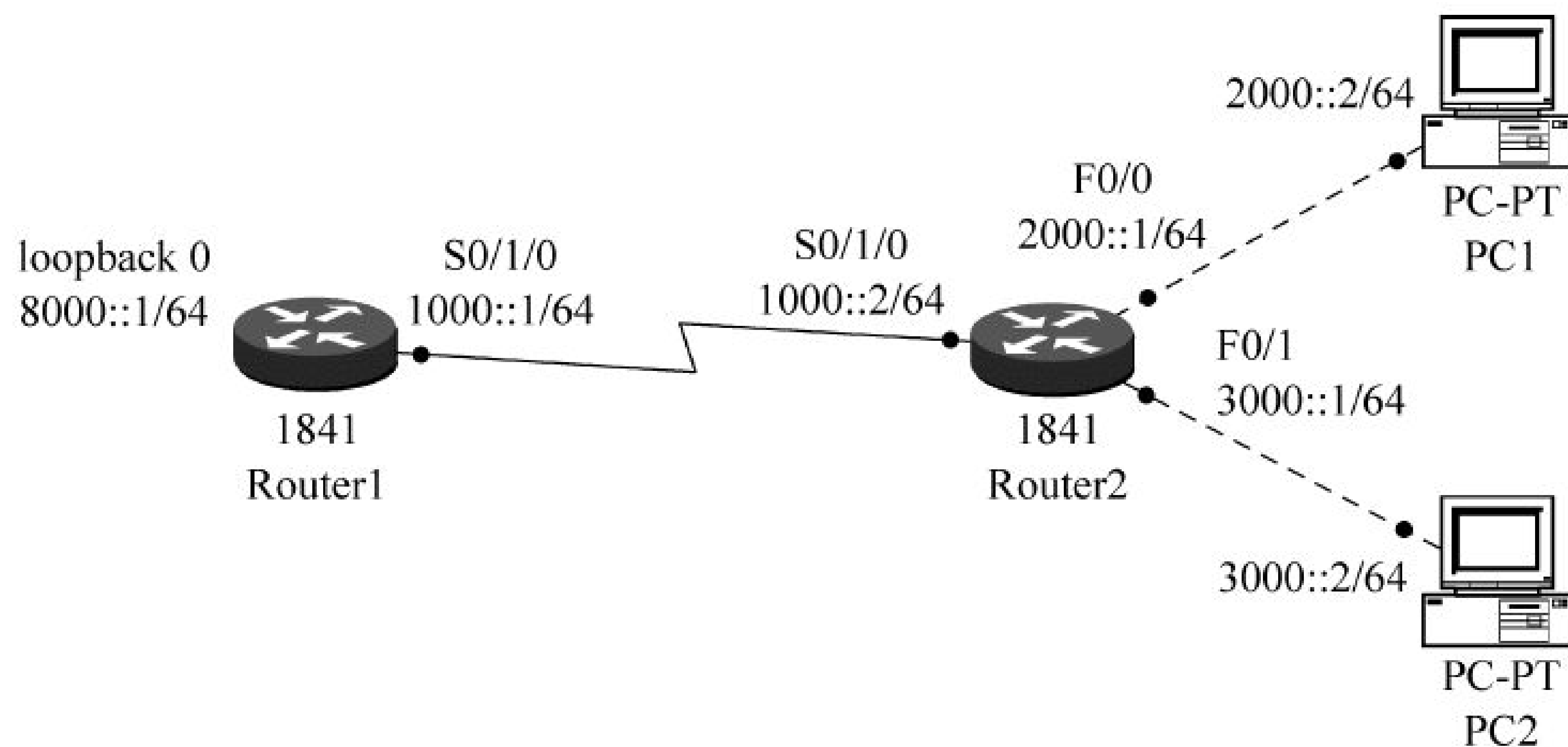


图 9-23 配置标准 IPv6 ACL 的网络环境

首先，配置路由器 Router1 的 IPv6 地址和 RIPng 协议，如图 9-24 所示。

```
Router1(config)#ipv6 unicast-routing
Router1(config)#ipv6 router rip test
Router1(config-rtr)#interface loopback 0
Router1(config-if)#ipv6 address 8000::1/64
Router1(config-if)#ipv6 rip test enable
Router1(config-if)#ipv6 enable
Router1(config-if)#interface s 0/1/0
Router1(config-if)#ipv6 address 1000::1/64
Router1(config-if)#ipv6 rip test enable
Router1(config-if)#ipv6 enable
Router1(config-if)#clock rate 128000
Router1(config-if)#no shutdown
Router1(config-if)#
```

图 9-24　配置路由器 Router1

在图 9-24 中，第 1 行命令的作用是使路由器 Router1 启用全局 IPv6 转发特性。

第 2 行命令的作用是指定路由器的协议为 RIPng 协议，进程名称为 test。

第 3 行命令的作用是定义环回接口 loopback 0。

第 4 行命令的作用是定义环回接口 loopback 0 的 IPv6 地址为 8000::1/64。

第 5、6 行命令的作用是在环回接口 loopback 0 启用 RIPng 协议进程 test。

第 7 行命令的作用是指定配置的接口为串行接口 s 0/1/0。

第 8 行命令的作用是指定串行接口 s 0/1/0 的 IPv6 地址为 1000::1/64。

第 9、10 行命令的作用是在串行接口 s 0/1/0 启用 RIPng 协议进程 test。

第 11 行命令的作用是指定串行接口 s 0/1/0 的时钟频率为 128000Hz。

第 12 行命令的作用是激活串行接口 s 0/1/0Hz。

同理，配置路由器 Router2 的 IPv6 地址和 RIPng 协议，如图 9-25 所示。各行命令的作用与图 9-25 相同，这里就不再详细说明了。

```
Router2(config)#ipv6 un
Router2(config)#ipv6 unicast-routing
Router2(config)#ipv6 router rip demo
Router2(config-rtr)#interface s 0/1/0
Router2(config-if)#ipv6 address 1000::2/64
Router2(config-if)#clock rate 128000
Router2(config-if)#no shutdown
Router2(config-if)#ipv6 rip demo enable
Router2(config-if)#ipv6 enable
Router2(config-if)#interface f 0/0
Router2(config-if)#ipv6 address 2000::1/64
Router2(config-if)#no shutdown
Router2(config-if)#ipv6 rip demo enable
Router2(config-if)#ipv6 enable
Router2(config-if)#interface f 0/1
Router2(config-if)#ipv6 address 3000::1/64
Router2(config-if)#no shutdown
Router2(config-if)#ipv6 rip demo enable
Router2(config-if)#ipv6 enable
Router2(config-if)#
```

图 9-25　配置路由器 Router2

接着，在路由器 Router1 上配置并应用一个名称为 MyACL 的标准 IPv6 ACL，如图 9-26 所示。

```
Router1(config)#ipv6 access-list MyACL
Router1(config-ipv6-acl)#deny ipv6 2000::/64 any Mask 1 any
Router1(config-ipv6-acl)#permit ipv6 any any Mask 1 any
Router1(config-ipv6-acl)#interface Serial 0/1/0
Router1(config-if)#ipv6 traffic-filter MyACL in
Router1(config-if)#
```

图 9-26　在路由器 Router1 上配置标准 IPv6 ACL

在图 9-26 中,第 1 行命令的作用是定义一个名称为 MyACL 的标准 IPv6 ACL,并进入 IPv6 ACL 配置子模式。

第 2 行命令的作用是指定过滤的条件,拒绝来自 IPv6 子网 2000::/64 的所有数据包。

第 3 行命令的作用是允许来自其他 IPv6 地址的所有数据包。

第 4 行命令的作用是指定当前要配置的接口。

第 5 行命令的作用是将名称为 MyACL 的标准 IPv6 ACL 应用在串行口 Serial 0/1/0 上,从而限制进入串行口 Serial 0/1/0 的数据包。

至此,标准 IPv6 ACL 配置完成。

此时,可以用 show access-list 命令查看配置成功的标准 IPv6 ACL,结果如图 9-27 所示。

```
Router1#show access-list
IPv6 access list MyACL
    deny ipv6 2000::/64 any (10 match(es))
    permit ipv6 any any (445 match(es))
Router1#
```

图 9-27　查看标准 IPv6 ACL

最后,在路由器 Router1 上用 ping 命令分别测试与 IPv6 子网 2000::/64 以及 IPv6 子网 3000::/64 的网络连通性。测试结果如图 9-28 所示。

```
Router1#ping 2000::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000::1, timeout is 2 sec
.....
Success rate is 0 percent (0/5)

Router1#ping 3000::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3000::1, timeout is 2 sec
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping 3000::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3000::2, timeout is 2 sec
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#
```

图 9-28　测试路由器 Router1 的网络连通性

图 9-28 表明，路由器 Router1 与子网 2000::/64 连接不通，而与子网 3000::/64 连接正常，即标准 IPv6 ACL 配置正确。

9.9.4 配置扩展 IPv6 访问控制列表

与 IPv4 一样，扩展 IPv6 ACL 基于源地址、目的地址、传输层协议、源端口、目的端口和其他 IP 特性允许或者拒绝数据包的策略。

1. 定义扩展 IPv6 ACL 的语法

```
access - list access - list - name {permit|deny} [protocol] [source - ipv6 - prefix/prefix - length|any|host host - ipv6 - address}[ eq | neq | lt | gt range source - port] {destination - ipv6 - prefix/prefix - length |any|host host - ipv6 - address] [eq|neq|lt|gt range destination - port][dscp value][flow - label value] [fragments] [routing] [undetermined - transport][reflect reflexive - access - list - name] [timeout value][time - range time - range - name] [log|log - input] [sequence value]
```

其中，定义扩展 IPv6 ACL 命令中各个参数的详细说明如下：

access-list-name(表名)：指定扩展 ACL 的名称。

permit：指定 IPv6 的允许条件；deny：指定 IPv6 的拒绝条件。

protocol(协议)：检查特定协议的数据包，如 TCP、UDP、ICMP、WWW 等协议。

source-ipv6-prefix/prefix-length：指定源 IPv6 地址前缀及前缀长度。

any：表示任何 IPv6 地址，与::/0 等价。

host host-ipv6-address：单个源 IPv6 地址，数据包来自这里。

destination-ipv6-prefix/prefix-length：指定目的 IPv6 地址前缀及前缀长度。数据包将发送到这个 IPv6 地址。

比较操作符 lt 表示小于；gt 表示大于；eq 表示等于；neq 表示不等于。range 用于指定范围。

dscp value、flow-label value、fragments、routing 和 undetermined-transport 这 5 个参数用于定义 IPv6 数据包头中特定字段进行匹配的值。

reflect reflexive-access-list-name：用于定义一个反射的 IPv6 ACL。

timeout value：指定反射的 IPv6 ACL 的超时时间值。

time-range time-range-name：指定一个基于时间的 IPv6 ACL。

log：这是一个可选项，用于生成 IPv6 日志，记录经过接口的数据包。

log-input：IPv6 访问列表日志记录的 log 关键字。使用这个关键字，只要可行，日志将会记录输入接口和源 MAC 地址。

2. 扩展 IPv6 ACL 的命令举例

下面举例说明常用的扩展 IPv6 ACL 的命令及其功能。

(1) Router(config)# ipv6 access-list DEMO

这个命令定义一个名字为 DEMO 的扩展 IPv6 ACL，并进入 IPv6 ACL 配置子模式。

(2) Router(config-ipv6-acl)# permit icmp any any router-advertisement

这个命令允许路由器从任何 IPv6 源地址向任何 IPv6 目的地址公告消息。

(3) Router(config-ipv6-acl)# permit icmp any anyrouter-solicitation

这个命令允许路由器从任何 IPv6 源地址向任何 IPv6 目的地址请求消息。

(4) Router(config-ipv6-acl)＃permit udp any host 2000::1 eq domain

这个命令允许 UDP 数据包从任何 IPv6 源地址到达 IPv6 地址为 2000::1 的目的主机。

(5) Router(config-ipv6-acl)＃permit tcp 3000::1/64 any reflect OUTGOING

这个命令允许 TCP 数据包从 IPv6 源地址 3000::1/64 到达任何目的 IPv6 网络的任何 TCP 端口。当匹配时,这个命令添加一个反射表项到 OUTGOING。

(6) Router(config-ipv6-acl)＃deny any 4000::1/64 routing

当有路由扩展包头时,这个命令拒绝来自任何 IPv6 源地址的数据包到达 IPv6 目的网络 4000::1/64。

(7) Router(config-ipv6-acl)＃deny any 5000::1/64 fragments

当有分段扩展包头时,这个命令拒绝来自任何 IPv6 源地址的数据包到达 IPv6 目的网络 5000::1/64。

(8) Router(config-ipv6-acl)＃deny any 6000::1/64 flow-label 100

当流标签字段等于 100 时,这个命令拒绝来自任何 IPv6 源地址的数据包到达 IPv6 目的网络 6000::1/64。

(9) Router(config-ipv6-acl)＃deny any any log

这个命令拒绝来自任何 IPv6 源地址的数据包到达任何 IPv6 目的地址,并在日志中保存记录。这个命令改写原来不保存的隐含规则 deny any any。

3. 配置扩展 IPv6 ACL 实例

下面以图 9-29 所示的网络环境为例,说明扩展 IPv6 ACL 的配置方法。

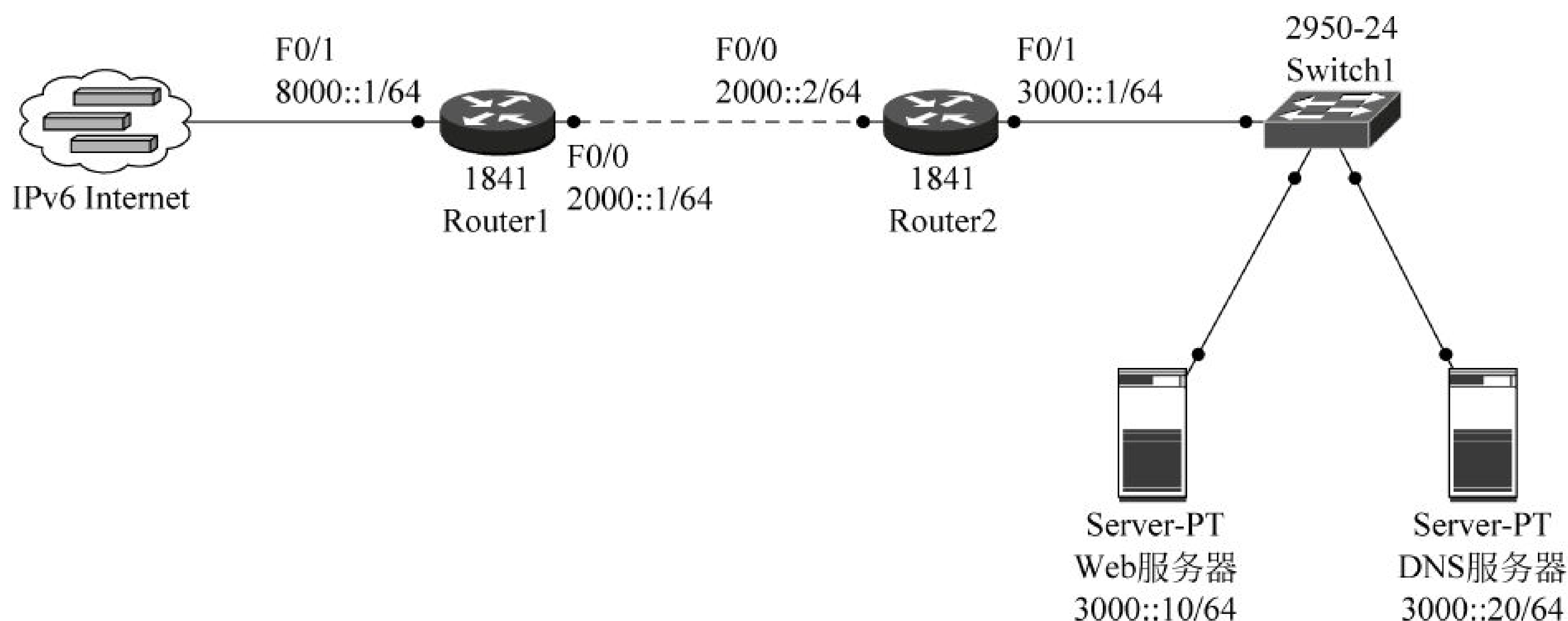


图 9-29 配置扩展 IPv6 ACL 的网络环境

首先,配置两个路由器的 IPv6 地址和 RIPng 协议,如图 9-30 和图 9-31 所示。

图 9-29 中,在 IPv6 地址 3000::10 的端口 80 上有一个 Web 服务器,在 IPv6 地址 3000::20 的端口 53 上有一个 DNS 服务器。假设 DNS 服务和 Web 服务可以被 IPv6 Internet 上任何地址访问,但是除了 ICMPv6 数据包以外,任何其他从 IPv6 Internet 进入的流量都被拒绝。在路由器 Router2 上配置扩展 IPv6 ACL 的步骤如图 9-32 所示。

在图 9-32 中,第 1 行命令定义一个扩展 IPv6 ACL,ACL 表名为 PUBLIC。

第 2 行命令允许任何 TCP 数据包从任何 IPv6 源地址到达目的主机 3000:10 的 80 端口,即允许在 IPv6 Internet 上的任何主机访问 Web 服务器 3000:10。

```
Router1(config)#ipv6 unicast-routing
Router1(config)#ipv6 router rip demo
Router1(config-rtr)#interface fastethernet 0/1
Router1(config-if)#ipv6 address 8000::1/64
Router1(config-if)#no shutdown
Router1(config-if)#ipv6 rip demo enable
Router1(config-if)#ipv6 enable
Router1(config-if)#interface fastethernet 0/0
Router1(config-if)#ipv6 address 2000::1/64
Router1(config-if)#no shutdown
Router1(config-if)#ipv6 rip demo enable
Router1(config-if)#ipv6 enable
Router1(config-if)#
```

图 9-30 配置路由器 Router1 的 IPv6 地址和 RIPng 协议

```
Router2(config)#ipv6 unicast-routing
Router2(config)#ipv6 router rip demo
Router2(config-rtr)#interface fastethernet 0/0
Router2(config-if)#ipv6 address 2000::2/64
Router2(config-if)#no shutdown
Router2(config-if)#ipv6 rip demo enable
Router2(config-if)#ipv6 enable
Router2(config-if)#interface fastethernet 0/1
Router2(config-if)#ipv6 address 3000::1/64
Router2(config-if)#no shutdown
Router2(config-if)#ipv6 rip demo enable
Router2(config-if)#ipv6 enable
Router2(config-if)#
```

图 9-31 配置路由器 Router2 的 IPv6 地址和 RIPng 协议

```
Router2(config)#ipv6 access-list PUBLIC
Router2(config-ipv6-acl)#permit tcp any host 3000::10 eq www
Router2(config-ipv6-acl)#permit tcp any host 3000::20 eq domain
Router2(config-ipv6-acl)#permit udp any host 3000::20 eq domain
Router2(config-ipv6-acl)#permit icmp any any
Router2(config-ipv6-acl)#deny ipv6 any any
Router2(config-ipv6-acl)#exit
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ipv6 traffic-filter PUBLIC in
Router2(config-if)#
```

图 9-32 配置路由器 Router2 的扩展 IPv6 ACL

第 3 行命令允许任何 TCP 数据包从任何 IPv6 源地址到达目的主机 3000:20 的 53 端口，即允许在 IPv6 Internet 上的任何主机访问 DNS 服务器 3000:20(DNS 响应)。

第 4 行命令允许任何 UDP 数据包从任何 IPv6 源地址到达目的主机 3000:20 的 53 端口，即允许在 IPv6 Internet 上的任何主机访问 DNS 服务器 3000:20(DNS 查询)。

第 5 行命令允许所有 ICMPv6 消息从任何 IPv6 源地址到达任何目的 IPv6 地址。

第 6 行命令拒绝从任何源 IPv6 地址到达任何目的地址的数据包。

第 7 行命令退出配置子模式。

第 8 行命令选择接口 fastethernet 0/0。

第 9 行命令将表名为 PUBLIC 的扩展 IPv6 ACL 应用于接口 fastethernet 0/0 来过滤进入的流量。

至此，扩展 IPv6 ACL 配置完成。验证方法与前面所述相同，这里不再赘述。

9.10 本章总结

访问控制列表(Access Control Lists,ACL)是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪些数据包可以收、哪些数据包需要拒绝。至于数据包是被接收,还是被拒绝,可以根据源地址、目的地址、端口号等的特定指示条件决定。

使用访问控制列表可以保护资源结点,阻止非法用户对资源结点访问,也可以限制特定用户结点的访问权限。例如,限制企业的人事部门使用 WWW 服务,就可以通过访问控制列表来实现;又如,为了企业会计部门的安全,既不允许会计部门的计算机访问外网,也不允许外网访问会计部门的计算机,这一特殊要求同样可以通过访问控制列表来实现。

访问控制列表是一组条件判断语句的集合,它定义了数据包进入路由器接口及通过路由器转发和流出路由器的行为。

目前,访问控制列表主要分为标准 ACL、扩展 ACL 和命名 ACL 3 大类。此外,还有基于时间的 ACL、IPv6 ACL 等。

标准 ACL 在路由器的全局配置模式下定义,其命令的语法格式是:

```
access-list access-list-number {permit|deny} source [source-wildcard] [log]
```

定义扩展 ACL 仍然使用 access-list 命令,在全局配置模式下使用,其命令格式如下:

```
access-list access-list-number {permit|deny} protocol source [source-wildcard]
destination [destination-wildcard] [operator operand] [established] [log]
```

定义命名 ACL 使用 ip access-list 命令,其语法格式如下:

```
ip access-list {standard|extended} name
```

基于时间的 ACL 可以在不同的时间段实施访问控制。在原有 ACL 的基础上应用时间段。时间段可以分为 3 种:绝对(absolute)时间段、周期(periodic)时间段和混合时间段。

定义标准 IPv6 ACL 使用 ipv6 access-list 命令,语法格式如下:

```
ipv6 access-list access-list-name
```

其中,access-list-name 是定义的标准 ACL 的表名。

在配置标准 IPv6 ACL 中,指定允许或拒绝数据包的条件使用以下命令:

```
permit|deny {source-ipv6-prefix/prefix-length | any | host host-ipv6-address}
{destination-ipv6-prefix/prefix-length | any | host host-ipv6-address}
```

定义扩展 IPv6 ACL 的语法格式如下:

```
access-list access-list-name {permit|deny} [protocol] [source-ipv6-prefix/prefix-
length|any|host host-ipv6-address}[ eq | neq | lt | gt range source-port] {destination-
ipv6-prefix/prefix-length |any|host host-ipv6-address] [eq|neq|lt|gt range destination-
port][dscp value][flow-label value] [fragments] [routing] [undetermined-transport][reflect
reflexive-access-list-name] [timeout value][time-range time-range-name] [log|log-
input] [sequence value]
```

复习思考题

1. 什么是访问控制列表?
2. 访问控制列表具有哪些功能?
3. 请画图说明访问控制列表的执行过程。
4. 访问控制列表分为哪些类型?
5. 如何配置标准访问控制列表? 如何配置扩展访问控制列表? 它们两者有何区别?
6. 如何配置命名的访问控制列表?
7. 如何配置基于时间的访问控制列表?
8. 如何配置标准 IPv6 访问控制列表? 如何配置扩展 IPv6 访问控制列表?

9. 实训操作题: 请按照图 9-33 所示的 IPv6 网络环境,在路由器 Router2 上配置扩展 IPv6 ACL,并测试配置的结果。

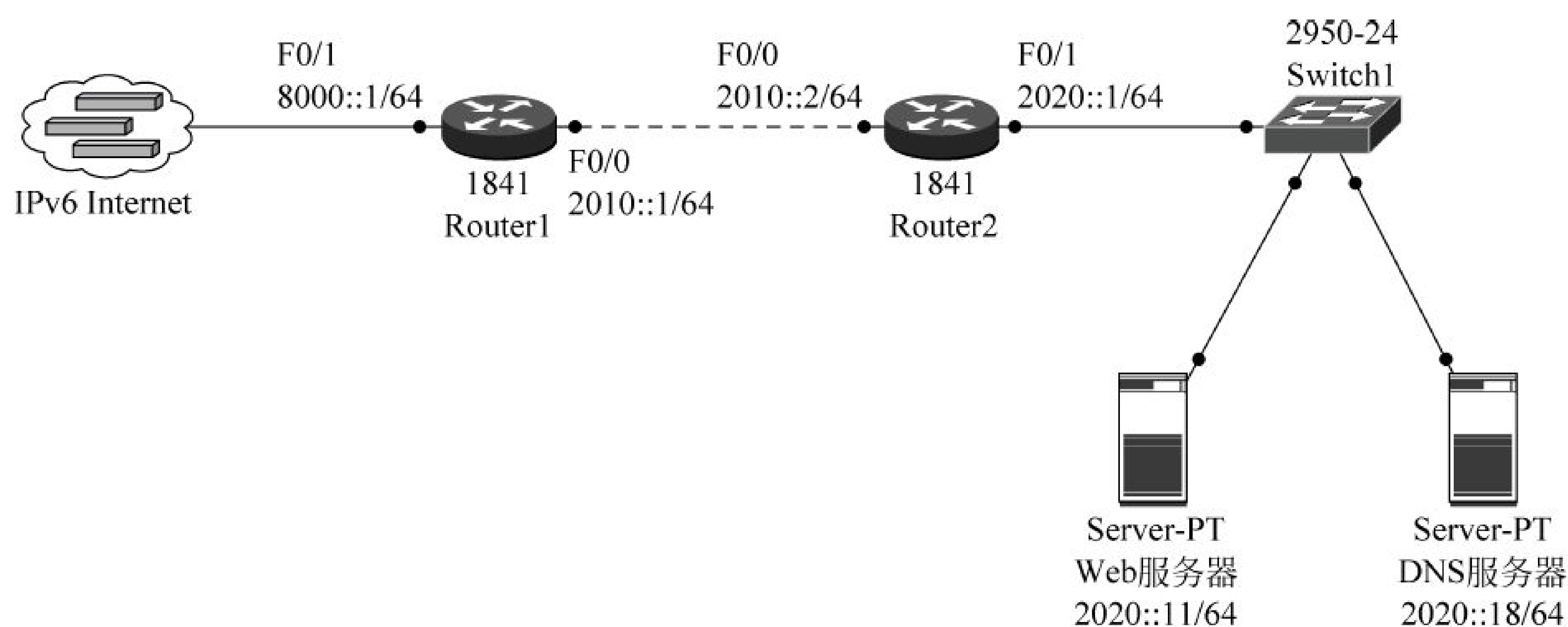


图 9-33 实训操作题的网络环境

在图 9-33 所示的网络环境中,IPv6 地址 2020::11 的端口 80 上有一个 Web 服务器,在 IPv6 地址 2020::18 的端口 53 上有一个 DNS 服务器。假设 DNS 服务和 Web 服务可以被 IPv6 Internet 上的任何地址访问,但是除了 ICMPv6 数据包以外,任何其他从 IPv6 Internet 进入的流量都被拒绝。

第 10 章 IPv6 过渡技术

CHAPTER 10

IP 地址的重要性是显而易见的，而能够提供海量的 IP 地址的 IPv6 技术则是下一代互联网（如移动互联网、物联网等）应用发展的基础。在我国目前 IPv4 地址已经严重不足的情况下，如何过渡到 IPv6 的问题就显得更为迫切。IPv6 采用 128 位地址格式，地址空间巨大，能够彻底解决 IPv4 地址不足问题。但是，由于 IPv6 与 IPv4 不兼容，因此在当前以 IPv4 为主的网络环境下，IPv4 向 IPv6 的平稳过渡就成为 IPv6 能否成功的关键。

虽然 IPv6 网络取代 IPv4 网络是一种必然的趋势，但是实现 IPv6 技术的全面应用仍然需要相当长的一段时间。也就是说，IPv4 是逐步过渡到 IPv6 的。过渡技术重点解决如何在 IPv4 网络环境里实现与 IPv6 网络的互操作及平滑过渡问题。

为了开展从 IPv4 到 IPv6 过渡问题和无缝互连问题的研究，国际互联网工程任务组（Internet Engineering Task Force，IETF）专门成立了一个工作组来处理这个问题。这个工作组就是下一代网络演进工作组（NGTRANS）。

目前已经提出了多种过渡技术和互连方案，这些技术各有特点，可以用于解决不同过渡时期、不同环境的 IPv4 与 IPv6 通信的问题。在过渡的初期，Internet 将由基于 IPv4 的“海洋”和基于 IPv6 的“小岛”组成。随着时间的推移，IPv4 的海洋将会逐渐缩小，而 IPv6 的小岛则会越来越多，最终完全取代 IPv4。

本章简要介绍目前比较成熟的从 IPv4 向 IPv6 过渡的技术。

10.1 过渡技术概述

目前，从 IPv4 过渡到 IPv6 的技术主要分为 3 大类：双协议栈技术、隧道技术和 IPv4/IPv6 协议转换技术。

1. 双协议栈技术

双协议栈（Dual Stack）技术就是指在一台设备上同时启用 IPv4 协议栈和 IPv6 协议栈。这样，这台设备既能和 IPv4 网络通信，又能和 IPv6 网络通信。如果这台设备是一个路由器，那么这台路由器的不同接口上分别配置了 IPv4 地址和 IPv6 地址，并很可能分别连接了 IPv4 网络和 IPv6 网络。如果这台设备是一个计算机，那么它将同时拥有 IPv4 地址和 IPv6 地址，并具备同时处理这两个协议地址的功能。

采用双协议栈技术的结点上同时运行着 IPv4 和 IPv6 两套协议栈。这是使 IPv6 结点保持与纯 IPv4 结点兼容最直接的方式，针对的对象是通信端结点（包括主机、路由器）。这

种方式对 IPv4 和 IPv6 提供了完全的兼容，但是对于 IP 地址耗尽的问题却没有任何帮助。由于需要双重路由基础设施，所以这种方式反而增加了网络的复杂度。

2. 隧道技术

隧道(Tunneling)技术是一种使用隧道在互联网中的通信双方之间传递特殊封装数据的技术。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将其他协议的数据帧或包重新封装，然后通过隧道发送。新的帧头提供路由信息，以便通过互联网传递被封装的负载数据。

隧道技术可以通过 IPv4 网络来实现两个 IPv6 站点之间的通信连接，反之，也可以通过 IPv6 网络实现两个 IPv4 站点之间的通信连接。

这里的隧道技术是指基于 IPv4 隧道来传送 IPv6 数据包的隧道技术。为了实现在 IPv4 海洋中传递 IPv6 数据包，可以将 IPv4 数据报文作为隧道载体，将 IPv6 报文整个封装在 IPv4 数据报文中，使 IPv6 报文能够穿透 IPv4 海洋到达另一个 IPv6 小岛。

为了便于读者理解隧道技术，打个比方，一个快递公司收件之后，发现目的地自己没有站点，无法投送，则将此包裹转交给能到达目的地的快递公司(如中国邮政)来投递。也就是说，将快递公司已经封装好的包裹(类似于 IPv6 报文)，外面用中国邮政的包装再封装一次(类似于封装成 IPv4 报文)，以便于这个包裹能在中国邮政的系统(IPv4 海洋)中被正常投递。

3. IPv4/IPv6 协议转换技术

IPv4/IPv6 协议转换技术提供了 IPv4 网络与 IPv6 网络之间的互访技术。网关路由器包含网络地址转换器(Network Address Translator - Protocol Translator，NAT-PT)，采用纯 IPv6 结点和 IPv4 结点间的互通方式工作，所有包括地址、协议在内的转换工作都由网关路由器来完成。

支持 NAT-PT 的网关路由器应具有 IPv4 地址池，供在从 IPv6 向 IPv4 域中转发包时使用，地址池中的地址用来转换 IPv6 报文中的源地址。此外，网关路由器需要 DNS-ALG 和 FTP-ALG 这两种常用的应用层网关的支持，在 IPv6 结点访问 IPv4 结点时发挥作用。如果没有 DNS-ALG 的支持，只能实现由 IPv6 结点发起的与 IPv4 结点之间的通信，反之则不行。如果没有 FTP-ALG 的支持，IPv4 网络中的主机将不能用 FTP 软件从 IPv6 网络中的服务器上下载文件或者上传文件，反之亦然。

NAT-PT 通过 IPv4 和 IPv6 数据报之间报头和语义的翻译，为 IPv6 结点与 IPv4 结点之间的通信提供透明的路由。它采用传统的 IPv4 下的 NAT 技术来分配 IPv4 地址，这样就可以用很少的 IPv4 地址构成自己的 IPv4 地址分配池，可以为大量的需要进行地址转换的应用提供服务。

10.2 双协议栈技术

10.2.1 双协议栈技术简介

双协议栈技术是指在网络结点上同时运行 IPv4 和 IPv6 两种协议，从而在 IP 网络中形成逻辑上相互独立的两个网络：IPv4 网络和 IPv6 网络。网络中的结点必须同时支持 IPv4 和 IPv6 协议栈，源结点根据目的结点的不同选用不同的协议栈，而网络设备根据报文的协议类型选择不同的协议栈进行处理和转发。双协议栈的工作原理如图 10-1 所示。

IPv4 应用层	IPv6 应用层
套接层	
TCP/UDP v4	TCP/UDP v6
IPv4	IPv6
数据链路层	
物理层	

图 10-1 双协议栈的工作原理

双协议栈技术是 IPv6 过渡技术中应用最广泛的一种过渡技术。同时,它也是所有其他过渡技术的基础。

采用双协议栈技术部署 IPv6,不存在 IPv4 和 IPv6 网络部署时相互影响的问题,可以按需部署。因此,双协议栈技术是部署 IPv6 网络最简单的方法,被国内外运营商广泛采用。双协议栈技术可以实现 IPv4 和 IPv6 网络的共存,但是不能解决 IPv4 和 IPv6 网络之间的互通问题。而且双协议栈技术既不能节省 IPv4 地址,也不能解决 IPv4 地址用尽的问题。

10.2.2 双协议栈关键技术

实现 IPv6 结点与 IPv4 结点互通的最直接的方式是在 IPv6 结点中加入 IPv4 协议栈。具有双协议栈的结点称为 IPv6/IPv4 结点,这些结点既可以收发 IPv4 报文,也可以收发 IPv6 报文。它们可以使用 IPv4 与其他 IPv4 结点互通,也可以使用 IPv6 与其他 IPv6 结点互通。

实现双协议栈方式要考虑的主要问题是地址,涉及双协议栈结点的地址配置和如何通过 DNS 获取通信对端的地址。

1. 双协议栈结点的地址配置

由于双协议栈结点同时支持 IPv4/IPv6,因此必须同时配置 IPv4 地址和 IPv6 地址。结点的 IPv4 地址和 IPv6 地址之间不必关联,但是对于支持自动隧道的双协议栈结点,必须配置与 IPv4 地址兼容的 IPv6 地址。

2. 通过 DNS 获取通信对端的地址

用户给应用层提供的只是通信对端的域名,而不是 IPv4 和 IPv6 地址,这就要求系统提供域名与地址之间的映射。无论是在 IPv4 网络中或在 IPv6 网络中,这个域名解析任务都是由 DNS 服务来完成的。对于 IPv6 地址,定义了新的记录类型 A6 和 AAAA。由于 IPv4/IPv6 结点要能够直接与 IPv4 和 IPv6 结点通信,因此必须提供对 IPv4 的 A 类记录及 IPv6 的 A6/AAAA 类记录的解析库。

然而,只提供解析库并不够,还必须对返回给应用层的地址类型进行选择。在查询到 IP 地址之后,解析库向应用层返回的 IP 地址可以有 3 种选择。

(1) 仅返回 IPv4 地址。

(2) 仅返回 IPv6 地址。

(3) 同时返回 IPv4 和 IPv6 地址。

对于前两种情况,应用层将分别使用 IPv4 或 IPv6 与对方进行通信;对于第三种情况,

应用层必须选择使用哪种地址，即使用哪种 IP。具体选择哪种地址与应用环境有关。

双协议栈技术、隧道技术和协议转换技术都要求在原有的结点上开发以下软件。

(1) ICMPv6 和邻居发现协议。

(2) 上层 TCP、UDP 对 IPv6 的处理程序。

(3) 修改与各种高层应用程序接口的套接库，以便支持 IPv6 地址和接口的扩充。

(4) 支持 IPv6 的 DNS 服务。

10.2.3 ICMPv6 简介

第 6 版的互联网控制信息协议(Internet Control Management Protocol Version 6，ICMPv6)，是为了与 IPv6 配套使用而开发的互联网控制信息协议。与 IPv4 一样，IPv6 也需要使用 ICMP，旧版本的 ICMP 不能满足 IPv6 全部要求，因此开发了新版本的 ICMP，即 ICMPv6。

ICMPv6 是 IPv6 的一个重要组成部分。ICMPv6 向源结点报告关于目的地址传输 IPv6 包的错误和信息，具有差错报告、网络诊断、邻结点发现和多播实现等功能。在 IPv6 中，ICMPv6 实现 IPv4 中 ICMP、ARP 和 IGMP 的功能。

互联网地址授权委员会(IANA)定义 ICMPv6 的协议号为 58。邻居发现(ND)协议和 NI 协议都基于 ICMPv6。ICMPv6 的主要功能如下。

1. 通告网络错误

例如，某台主机或整个网络由于某些故障不可达，又如指向某个端口号的 TCP 报文没有收到接收方的确认，这些错误信息都由 ICMPv6 报告。

2. 通告网络拥塞

当路由器缓存太多包，由于传输速度无法达到它们的接收速度，将会生成“ICMPv6 源结束”信息。对于发送方，这些信息将会导致传输速度降低。当然，更多的 ICMPv6 源结束信息的生成也将引起更多的网络拥塞。

3. 协助解决故障

ICMPv6 支持 Echo 功能，即在两个主机间一个往返路径上发送一个包。ping 是一种基于这种特性的网络连通性测试工具，它将传输一系列的包，测量平均往返次数并计算丢失百分比。

4. 通告超时

如果一个 IPv6 数据包的 TTL 降低到零，路由器就会丢弃此包，这时会生成一个 ICMPv6 信息包通告这一事实。TraceRoute 是一个路由追踪工具，它通过发送小 TTL 值的 ICMPv6 信息包并监视 ICMPv6 的超时状况，通告追踪可达的 IPv6 路由。

10.2.4 邻居发现协议简介

邻居发现协议(Neighbor Discovery Protocols，NDP)是为 IPv6 开发的邻居发现协议，由 RFC2461 定义，它可以使结点(主机和路由器)发现本链路上其他邻居的数据链路层地址。主机可以使用邻居发现协议发现邻近的路由器，把它作为自己的默认网关；结点使用邻居发现协议主动跟踪邻居是否可达，并检测邻居数据链路层地址的改变。当路由器或到达路由器的路径失效时，主机依靠该协议主动搜索可用的路由器或路径。概括起来，邻居发现协议解决的是在统一链路上的结点之间的交互问题。

IPv6 邻居发现协议是用来替代 IPv4 中的 ARP 的，用于实现网络层地址与链路层地址之间的映射。NDP 的工作效率比 ARP 高。

1. IPv6 邻居发现协议的功能

IPv6 邻居发现协议可以提供以下功能：

(1) 无服务器的自动配置。

(2) 路由发现。

(3) 地址解析。

(4) 邻居不可达检测。

(5) 链路 MTU(最大传输单元)发现。

(6) 下一跳决定。

(7) 重复地址检测。

2. 邻居发现协议数据包的类型

邻居发现协议定义了 5 五种类型的数据包，分别是路由器请求、路由器公告、邻居请求、邻居公告和重定向。

(1) 路由器请求(Router Solicitation，RS)，当结点不愿意等到下一次周期性的路由器公告时，可发起一次路由器请求的多播包。正在初始化的结点可使用路由器请求，这样即可得到路由相关参数。

(2) 路由器公告(Router Advertisement，RA)，路由器可周期性地发送路由器公告包，这样链路内的结点就可获得相关的路由配置信息。路由器公告包的跳数限制为 255，防止非本链路的路由发送路由器公告包来干扰本链路的通信。

(3) 邻居请求(Neighbor Solicitation，NS)，用于确定邻居的链路层地址，判断缓存中的链路层地址是否可达，判断链路中是否存在重复的 IP 地址。这里的跳数限制仍然为 25，防止邻居请求包通过路由器。

(4) 邻居公告(Neighbor Advertisement，NA)，一种情况是应答邻居请求，另一种情况是当结点发生改变时，发送多播包给本链路中的结点通知链路层地址改变信息。

(5) 重定向(Redirect)，由路由器发送，用于把数据包重定向到两路中链路质量更好的结点。

IPv6 中通过邻居请求，邻居公告实现了原来 IPv4 中的 ARP 功能。因为 ARP 采用了广播的形式，耗费资源更多，所以实现起来没有路由发现协议效率高。

10.2.5 支持 IPv6 的 DNS 简介

域名系统(Domain Name System，DNS)是国际互联网必不可少的重要组成部分，是互联网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便地通过域名访问互联网，而不用去记住难以记忆的 IP 地址。通过域名或主机名，最终得到该域名或主机名对应的 IP 地址的过程叫作域名解析(或主机名解析)。DNS 协议运行在 UDP 之上，使用端口号 53。在 RFC 文档中，RFC 2181 对 DNS 有规范说明，RFC 2136 对 DNS 的动态更新进行说明，RFC 2308 对 DNS 查询的反向缓存进行说明。

1. DNS 的功能

每个 IP 地址都可以有一个主机名，主机名由一个或多个字符串组成，字符串之间用小数点隔开。有了主机名，就不要死记硬背每台 IP 设备的 IP 地址，只要记住相对直观有意义

的主机名就行了。这就是 DNS 协议要完成的功能。

主机名到 IP 地址的映射有静态映射和动态映射两种方式。

1）静态映射

每台设备上都配置主机到 IP 地址的映射，各设备独立维护自己的映射表，而且只供本设备使用。

2）动态映射

建立一套域名解析系统，只在专门的 DNS 服务器上配置主机到 IP 地址的映射，网络上需要使用主机名通信的设备，首先需要到 DNS 服务器查询主机对应的 IP 地址。

通过主机名，最终得到该主机名对应的 IP 地址的过程叫作域名解析（或主机名解析）。在解析域名时，可以首先采用静态域名解析的方法，如果静态域名解析不成功，再采用动态域名解析的方法。可以将一些常用的域名放入静态域名解析表中，这样可大大提高域名解析效率。

2. DNS 服务器

DNS 服务器是安装了 DNS 服务器端软件的计算机。服务器端软件既可以是基于类 Linux 操作系统的，也可以是基于 Windows NT 系列操作系统的。安装好 DNS 服务器软件后，就可以实现域名解析服务了。

3. DNS 服务器冗余

为保证服务的高可用性，DNS 要求使用多台名称服务器冗余支持每个区域。某个区域的资源记录通过手动或自动方式更新到单个主名称服务器（称为主 DNS 服务器）上，主 DNS 服务器可以是一个或几个区域的权威名称服务器。其他冗余名称服务器（称为辅 DNS 服务器）用作同一区域中主服务器的备份服务器，以防主服务器无法访问或宕机。辅 DNS 服务器定期与主 DNS 服务器通信，确保它的区域信息保持最新。如果不是最新信息，辅 DNS 服务器就会从主服务器获取最新区域数据文件的副本。这种将区域文件复制到多台名称服务器的过程称为区域复制。

10.2.6 在路由器上配置双协议栈

在一个支持 IPv6 的路由器上配置双协议栈的方法很简单，只要同时在同一个网络接口上分配 IPv4 地址和 IPv6 地址即可。此后，路由器就能够同时转发 IPv4 和 IPv6 数据包了。

下面以图 10-2 所示的最简单的网络环境为例，介绍双协议栈的配置方法。



图 10-2 配置双协议栈的网络环境

这里，要为路由器 Router1 的同一个网络接口 fastethernet 0/0 同时配置 IPv6 地址 3FFE:2000::1/64 和 IPv4 地址 202.101.10.1；还要为路由器 Router2 的同一个网络接口 fastethernet 0/0 同时配置 IPv6 地址 3FFE:2000::2/64 和 IPv4 地址 202.101.10.2。为路由器 Router1 和路由器 Router2 配置双协议栈的命令分别如图 10-3 和图 10-4 所示。

```
Router1(config)#ipv6 unicast-routing
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ipv6 address 3FFE:2000::1/64
Router1(config-if)#ipv6 enable
Router1(config-if)#ip address 202.101.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#
```

图 10-3　为路由器 Router1 配置双协议栈

```
Router2(config)#ipv6 unicast-routing
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ipv6 address 3FFE:2000::2/64
Router2(config-if)#ipv6 enable
Router2(config-if)#ip address 202.101.10.2 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#
```

图 10-4　为路由器 Router2 配置双协议栈

至此，双协议栈配置完成。此时，可以在两个路由器的特权模式上分别用 ping 命令测试 IPv6 和 IPv4 网络的连通性，结果如图 10-5 所示。

```
Router1#ping 3FFE:2000::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3FFE:2000::2, timeout is
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#ping 202.101.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.101.10.2, timeout is
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#
```

图 10-5　测试网络连通性

图 10-5 表明，在路由器 Router1 的网络接口 fastethernet 0/0 上，IPv6 和 IPv4 与路由器 Router2 的网络接口 fastethernet 0/0 都连通正常。

10.3　隧道技术

隧道技术是通过将 IPv6 数据包封装在 IPv4 数据包中，然后将携带了 IPv6 数据的 IPv4 数据包在 IPv4 隧道中进行传输，到接收端再解封，还原为 IPv6 数据包。隧道技术的工作原理如图 10-6 所示。

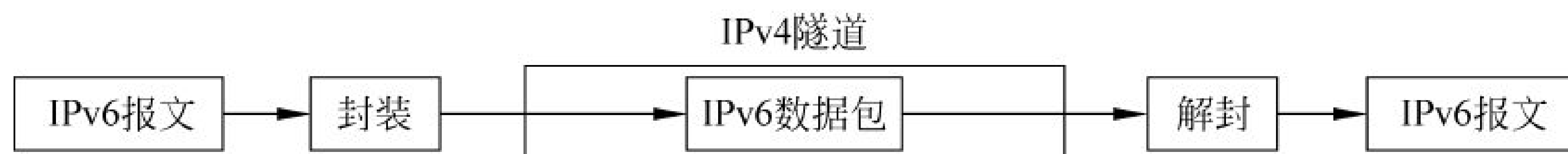


图 10-6　隧道技术的工作原理

隧道技术的优点是：不用把所有的网络设备都升级为双协议栈，只要求 IPv4/IPv6 网络的边缘设备实现双协议栈和隧道功能。除了边缘结点以外，其余结点都不需要支持双协议栈。

隧道技术本质上仅是提供一个点到点的透明传送通道，无法实现 IPv4 结点和 IPv6 结点之间的通信，适用于同协议类型网络孤岛之间的互联。

隧道的类型有多种，根据隧道协议的不同来分，可以将隧道分为 IPv4 over IPv6 隧道和 IPv6 over IPv4 隧道；根据隧道终点地址的获得方式来分，可以将隧道分为配置型隧道（如手动配置隧道、GRE 隧道）和自动配置的兼容隧道（如 6over4、6to4、6RD、ISATAP、Teredo、隧道代理等）。

本节将简要介绍几种常用的隧道技术。

10.3.1 手动配置隧道

手动配置隧道（Manually Configured Tunnel，RFC 2893）是通过 IPv4 骨干网连接的两个 IPv6 域的一条永久链路，这条永久链路用于两个边缘路由器或终端系统与边缘路由器之间定期安全通信的稳定连接。手动配置隧道适用于两台边缘路由器或者边缘路由器和主机之间对安全性要求比较高并且比较固定的连接上。

当配置手动隧道时，网络管理员需要手动配置隧道接口的 IPv6 地址，并且也必须手工配置隧道的源 IPv4 地址（Tunnel Source）和目的 IPv4 地址（Tunnel Destination）。隧道两端的路由器必须同时支持 IPv6 和 IPv4 协议栈。手工配置隧道在实际应用中总是成对配置的，即在两台边缘路由器上同时配置，因此，手工配置隧道是一种点对点的隧道。

隧道的配置需要隧道两个端点所在网络的管理员协作完成。隧道的端点地址由管理员手动配置来决定，不需要为站点分配特殊的 IPv6 地址，适用于经常通信的 IPv6 之间。每个隧道的封装结点必须保存隧道终点地址，当一个 IPv6 数据包在隧道上传输时，终点地址会作为 IPv4 数据包的目的地址进行封装。通常，封装结点要根据路由信息来决定一个数据包是否要通过隧道转发。

采用手动配置隧道进行通信的站点必须有可用的 IPv4 连接，并且至少要具有一个全球唯一的 IPv4 地址。站点中的每个主机都需要支持 IPv6，路由器需要支持双协议栈。在隧道要经过 NAT 设施的情况下，隧道机制不可用。

手动配置隧道的主要缺点是网络管理员的负担很重，因为要为每条隧道进行详细的配置。

10.3.2 GRE 隧道

RFC 2784 定义了一种更通用的隧道机制，即通用路由封装（Generic Routing Encapsulation，GRE）。GRE 隧道机制提出了如何用一种网络协议去封装另一种网络协议的技术方案，包括使用 IP 报文、网际包交换（IPX）协议、AppleTalk 报文等。

GRE 隧道是一种能够保证稳定和安全的端到端链路的标准隧道技术。GRE 隧道可以在 IPv4 隧道上承载 IPv6 报文。Cisco iOS 技术支持 IPv6 数据包的 GRE 封装。和手动配置隧道一样，GRE 隧道必须在允许通过现有的 IPv4 隧道传输 IPv6 数据包的路由器之间静态配置。

GRE隧道是一种点对点的隧道，隧道的起点和终点都需要手工配置。GRE把IPv6作为乘客协议，把GRE作为承载协议。配置基于IPv4的GRE隧道的边缘路由器和终端系统必须实现双协议栈，在IPv4的GRE隧道上承载IPv6数据报，IPv6地址是在Tunnel接口上配置，IPv4地址是Tunnel的起始地址和终点地址。所有要通过IPv4网络转发到IPv6网络的IPv6报文通过隧道入口封装为GRE格式，然后再封装在IPv4数据包中，在出口解封为IPv6数据包。当数据包封装为GRE格式后，目的地址就是隧道出口的IPv4地址。

与其他隧道协议不同，GRE需要使用特殊的隧道首部。在IPv6过渡场景中，GRE隧道报文的封装格式如图10-7所示。

IPv4首部	GRE首部	IPv6首部	IPv6载荷

图10-7　GRE隧道报文的封装格式

GRE隧道报文首先在IPv6首部添加一个GRE首部，再把整个数据包作为IPv4报文的有效数据部分封装在IPv4报文中，而IPv4报文的源地址和目的地址都是在GRE隧道接口配置中手动指定的。手动的GRE隧道并不适用于大量部署，一般只用于隧道端点相对固定的场景中。RFC 2784定义的GRE首部的格式如图10-8所示。

<table>
<tr><td>C</td><td>保留</td><td>版本</td><td>协议类型</td></tr>
<tr><td colspan="3">校验和(可选)</td><td>保留(可选)</td></tr>
</table>

图10-8　RFC 2784定义的GRE首部的格式

在图10-8中，标识位C用于标志可选的校验和是否存在，协议类型指明了GRE隧道承载的是什么协议，当用于承载IPv6时，协议类型为41。校验和的计算包括了GRE首部和有效数据载荷部分。当GRE用于IPv6过渡场景时，承载协议IPv4的首部中的协议号为47，标志着下一个协议类型为GRE协议。

10.3.3 自动配置的兼容隧道

RFC 2893定义了自动配置的兼容隧道(Auto-configured Tunnel)机制。自动配置的兼容隧道的建立和拆除是自动的，并且是动态实现的。自动配置的兼容隧道的端点根据数据包的目的地址确定，适用于单独的主机之间或不经常通信的站点之间。自动配置的兼容隧道需要站点采用与IPv4兼容的IPv6地址(IPv4 Compatible IPv6 address)，即0::a.b.c.d/96，其中，a.b.c.d是IPv4地址。这些站点之间必须有可用的IPv4连接，每个采用这种机制的主机都需要有一个全球唯一的IPv4地址。采用这种机制不能解决IPv4地址空间耗尽的问题。另外，还有一种危险就是如果把Internet上的全部IPv4路由表都包括到IPv6网络中，则会加剧路由表膨胀的问题。这种隧道的两个端点都必须支持双协议栈。当隧道要经过NAT(网络地址转换)设备的情况下，这种机制不可用。

10.3.4 6over4隧道

RFC 2529定义的IPv4组播隧道(6over4)是一种自动建立隧道的机制，这种隧道端点的IPv4地址采用邻居发现的方法来确定。与手动配置隧道不同的是，它不需要任何地址配

置；与自动配置的兼容隧道不同的是，6over4 隧道不要求使用 IPv4 兼容的 IPv6 地址。但是，采用这种机制的前提是 IPv4 网络基础设施须支持 IPv4 组播。

6over4 是一种 IPv4 组播隧道机制，通过将 IPv6 数据包封装在 IPv4 中的方式连接互相分离的 IPv6 主机。6over4 主机的 IPv6 地址由 64 位的单播地址前缀和规定格式的 64 位接口标识符：AABB:CCDD 组成，其中 AABB:CCDD 是其 IPv4 地址 a. b. c. d 的十六进制表示。6over4 将 IPv4 网络当作具有组播功能的一条链路，通过 IPv6 组播地址和 IPv4 组播地址的映射关系实现 IPv6 的邻居发现功能，因此，它要求 IPv4 网络支持组播功能。实际的 IPv4 网络很少支持组播功能，所以 6over4 隧道极少使用。

10.3.5 6to4 隧道

RFC 3056 定义的 6to4 也是一种自动构造隧道的机制，这种机制要求站点采用特殊的 IPv6 地址，即 2002:a. b. c. d::/48，其中，a. b. c. d 是相应的 IPv4 地址。这种特殊地址是自动从站点的 IPv4 地址派生出来的。所以，每个采用 6to4 机制的结点必须具有一个全球唯一的 IPv4 地址，这种地址分配方法可以使得其他域的边界路由器自动地区分隧道接收端点是否在本域内。因为这种机制下隧道端点的 IPv4 地址可以从 IPv6 地址中提取，所以隧道的建立是自动的。6to4 隧道不会在 IPv4 的路由表中引入新的条目，在 IPv6 的路由表中只增加一条表项。采用 6to4 机制的 ISP 只需要做很少的管理工作，因此这种机制非常适用于运行 IPv6 的站点之间的通信。6to4 机制要求隧道中至少有两台路由器支持双协议栈和 6to4，主机要求支持 IPv6 协议栈。

6to4 机制把广域的 IPv4 网络作为一个单播的点对点链路层。这种机制适合作为 IPv4/IPv6 共存的初始阶段的转换工具，它可以与防火墙、NAT 技术共存，但是 NAT 设备必须具有全球唯一的 IPv4 地址，并且应有 6to4 机制和完备的路由功能。

10.3.6 6RD 隧道

6RD 是 IPv6 快速部署(IPv6 Rapid Deployment)的简称，其对应的标准为 RFC 5569。6RD CE 隧道技术是由法国运营商 FREE 提出的。FREE 在提出该方案的短短 5 周内就已经为超过 150 万户用户提供了 IPv6 服务。6RD BR 是在 6to4 基础上发展起来的一种 IPv6 网络过渡技术方案。通过在现有 IPv4 网络中增加 6RD-BR，给愿意使用 IPv6 的用户提供 IPv6 接入；在 IPv6 用户的家庭网关和 6RD 网关之间建立 6in4 隧道，从而实现在 IPv4 网络提供 IPv6 服务的能力。

6RD 的网络结构如图 10-9 所示。在图 10-9 中，用户边缘设备(Customer Edge，CE) 6RD 与边界中继器(Border Relay，BR)6RD 都是双协议栈设备，通过扩展的 DHCP 选项，6RD CE 的 WAN 接口得到运营商为其分配的 IPv6 前缀、IPv4 地址(公有或私有)以及 6RD BR 的 IPv4 地址等参数。CE 在 LAN 接口上通过将上述 6RD IPv6 前缀与 IPv4 地址拼接构造出用户的 IPv6 前缀。当用户开始发起 IPv6 会话，IPv6 报文到达 CE 后，CE 用 IPv4 包头将其封装进隧道，被封装的 IPv6 报文通过 IPv4 包头进行路由，中间的设备对其中的 IPv6 报文不感知。BR 作为隧道边界的中继设备，收到 IPv4 数据包后进行解封装，将解封装后的 IPv6 报文转发到全球 IPv6 网络中，从而实现终端用户对 IPv6 业务的访问。

6RD 对运营商的核心网络影响极小，整个过程呈透明状态。它为运营商在 IPv6 过渡

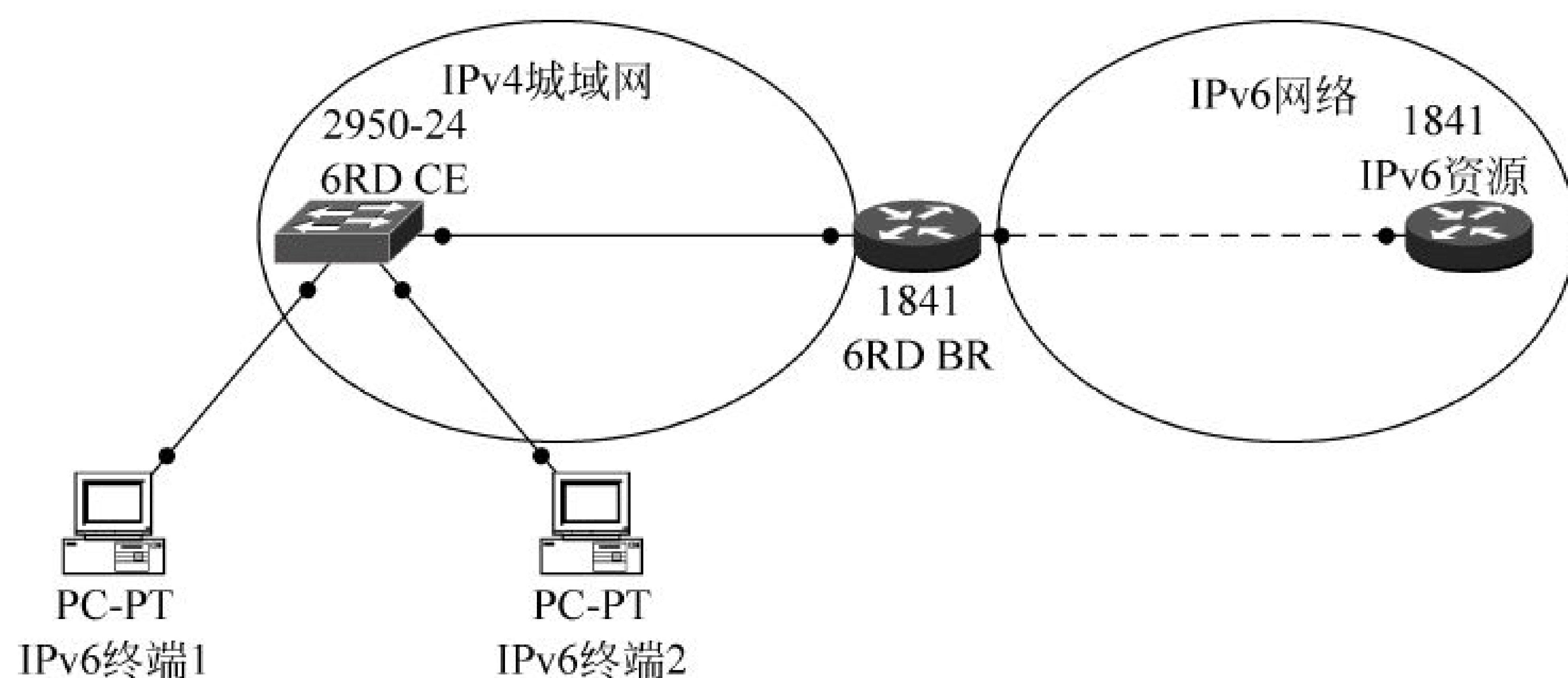


图 10-9　6RD 的网络结构

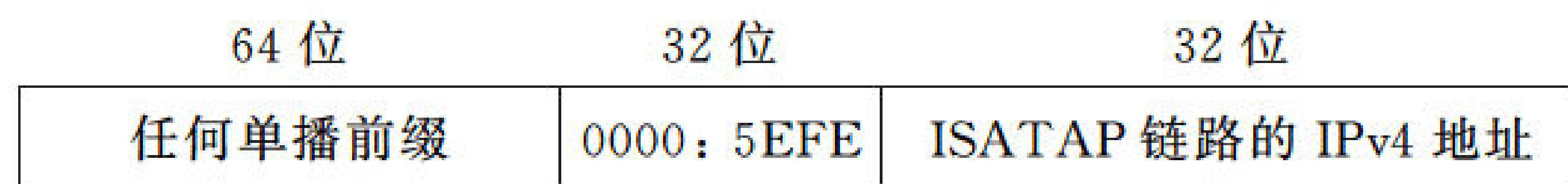
初期引入 IPv6 服务提供了思路。在这种方案中，需要同时为终端分配 IPv6 前缀和 IPv4 公有/私有地址，仍不能减少 IPv4 地址的消耗。由于 IPv6 地址前缀受 IPv4 地址的影响，所以该方案也存在 IPv6 地址欺骗的缺点；同时，该方案也要求分配给 CE 的 IPv4 地址有较长的租用期。

10.3.7　ISATAP 隧道

站内自动隧道寻址协议(ISATAP)是一种地址分配和主机到主机、主机到路由器和路由器到主机的自动隧道技术，它为 IPv6 主机之间提供了跨越 IPv4 内部网络的单播 IPv6 连通性。ISATAP 一般用于 IPv4 网络中的 IPv6/IPv4 结点间的通信。

ISATAP 是一种站点内部的 IPv6 体系架构将 IPv4 网络视为一个非广播型多路访问(NBMA)链路层的 IPv6 隧道技术，即将 IPv4 网络当作 IPv6 的虚拟链路层。ISATAP 主要用于当一个站点内部的纯 IPv6 网络还不能用，但是又要在站点内部传输 IPv6 报文的情况。例如，站点内部有少数测试用的 IPv6 主机要互相通信。使用 ISATAP 隧道允许站点内部同一虚拟链路上的 IPv4/IPv6 双协议栈主机互相通信。

ISATAP 使用的 IPv6 地址的前缀可以是任何有效的 IPv6 单播前缀、包括全局地址前缀、链路的本地前 64 位前缀和站点本地前缀，IPv4 地址被放置在最后 32 位的 IPv6 地址，使得隧道可以自动形成。ISATAP 隧道的地址结构如图 10-10 所示。



64 位	32 位	32 位
任何单播前缀	0000：5EFE	ISATAP 链路的 IPv4 地址

图 10-10　ISATAP 隧道的地址结构

ISATAP 使用本地管理的接口标识符：:0:5EFE:w. x. y. z，其中：:0:5EFE 部分是由 Internet 号码分配中心(IANA)分配的机构单元标识符(00-00-5E)和表示内嵌的 IPv4 地址类型的类型号(FE)组合而成的。w. x. y. z 部分是任意的单播 IPv4 地址，既可以是私有地址，也可以是公共地址。

例如，IPv6 的前缀是 2001::/64，嵌入的 IPv4 的地址是 192.168.1.1，在 ISATAP 地址中，IPv4 地址 192.168.1.1 用十六进制数表示为 C0A8:0101，因此其对应的 ISATAP 地址为 2001::0000:5EFE:C0A8:0101。

ISATAP 隧道是一种成熟的 IPv6 过渡技术。在一个 IPv4 网络中，可以非常轻松地进

行ISATAP隧道的部署。首先，主机必须是支持IPv4/IPv6双协议栈的计算机，然后，需要有一台支持ISATAP的路由器，ISATAP路由器可以配置在IPv4网络中的任何位置，只要主机能够ping通它即可。当然，需要知道ISATAP路由器的IPv4地址。接着就可以在路由器上部署ISATAP了。这样，网络中支持ISATAP的双协议栈主机在需要访问IPv6资源时，就可以与ISATAP路由器建立起ISATAP隧道，ISATAP主机根据ISATAP路由器下发的IPv6前缀构造自己的IPv6地址(这个IPv6地址被自动关联到ISATAP主机本地产生的一个ISATAP虚拟网卡上)，并且将这台ISATAP路由器设置为自己的IPv6默认网关，如此一来，后续的这台主机就能够通过这台ISATAP路由器去访问IPv6的资源了。

这种方法部署起来非常简单，在许多场合，客户为了节省成本，又希望网络中的IPv6主机能够访问V6资源，同时又不愿意对现有网络做大规模的变更及设备升级，那么就可以采用这种方法，购买一台支持ISATAP的路由器，甚至可以将ISATAP路由器旁挂在网络上，只要它能够访问V6资源并且响应ISATAP个人计算机的隧道建立请求。

10.3.8 Teredo隧道

Teredo隧道是一种IPv6 over UDP隧道。因为传统的NAT技术不能支持IPv6 over IPv4数据包的穿越，所以，为了解决这个问题，采用把IPv6数据包封装在UDP载荷中的方式穿过NAT。

Teredo协议中定义了4种不同的实体：Client、Server、Relay、Host-specific Relay。其中，Client是指处于NAT域内并想要获得IPv6全球连接的主机，Server具有全球地址并且能够为Client分配Teredo地址，Relay负责转发Client和一般IPv6结点通信时的数据包，Host-specific Relay是指不通过Relay就可以直接和Client进行通信的IPv6主机。这些角色都同时支持IPv4/IPv6。

Teredo隧道的地址结构如图10-11所示。

前缀	IPv4服务器	标志	接口	IPv4客户端
Prefix	Server IPv4	Flags	Port	Client IPv4

图10-11 Teredo隧道的地址结构

Teredo隧道又称为面向IPv6的IPv4 NAT网络地址转换穿越，是一项IPv6/IPv4过渡技术，在IPv6/IPv4主机位于一个或多个IPv4 NAT之后时，用来为单播IPv6连接提供地址分配和主机间的自动遂道。来自Teredo主机的IPv6数据流能够通过NAT，因为它是以IPv4 UDP数据格式发送的。如果NAT支持UDP端口解析，那么它就支持Teredo。

Teredo是作为实现IPv6连接最后一种转换技术而设计的，认识到这一点很重要。如果原来的IPv6、6to4或者ISATAP连接可用，那么主机就不必作为Teredo的客户端。越来越多的IPv4 NAT经过了升级，以便能够支持6to4，而且IPv6连接变得越来越普遍，Teredo将会使用得越来越少，直到最后完全被放弃。

10.3.9 隧道代理技术

RFC 3053定义的隧道代理(Tunnel Broker)并非一种隧道机制，而是一种方便构造隧道的机制。这种机制可以简化隧道的配置过程，适用于单个主机获取IPv6连接的情况。隧

道代理也可用于站点之间，但这时有可能会在 IPv6 的路由表中引入很多条目，而导致 IPv6 的路由表过于宠大，违背 IPv6 设计的初衷。用户可以通过隧道代理从支持 IPv6 的 ISP 处获得持久的 IPv6 地址和域名。隧道代理要求隧道的双方都支持双协议栈并有可用的 IPv4 连接，在隧道要经过 NAT 设施的情况下，这种机制不可用。采用隧道代理的方法，可以使 IPv6 的 ISP 很容易地对用户执行接入控制，按照策略对网络资源进行分配。

隧道代理是一种架构，而不是具体的网络协议，其结构如图 10-12 所示。

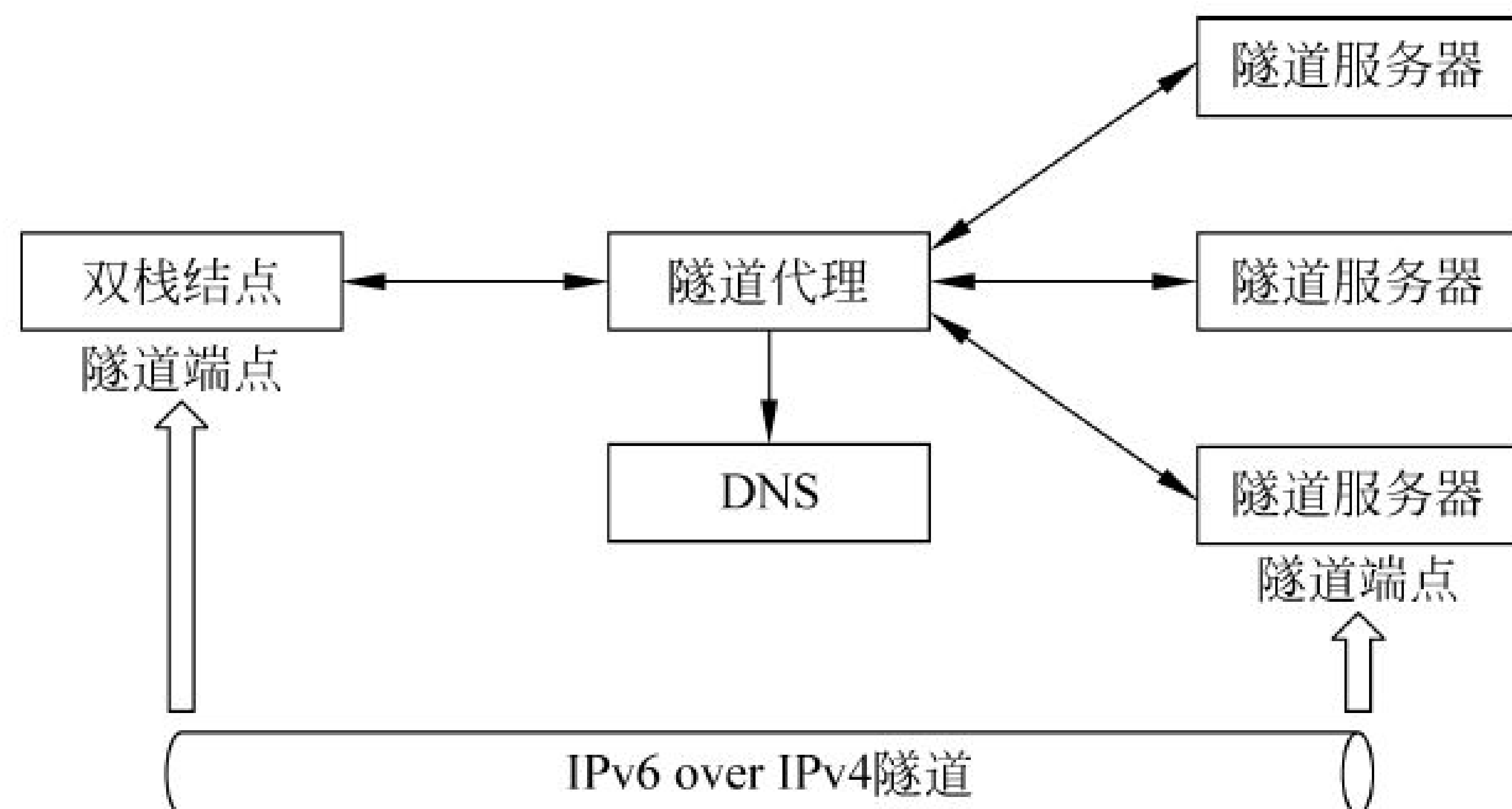


图 10-12 隧道代理的结构

隧道代理的主要目的是简化隧道的配置，提供自动的配置手段。从这个意义上说，隧道代理可以看作是一个虚拟的 IPv6 ISP，通过 Web 方式为用户分配 IPv6 地址，建立隧道，以提供和其他 IPv6 站点的通信。隧道代理的特点是灵活、可操作性强，针对不同用户可提供不同的隧道配置。

隧道代理的工作过程是：客户端首先到隧道代理(Tunnel Broker)处注册，隧道代理为用户选择隧道服务器(Tunnel Server)，为用户选择前缀等配置信息，并将隧道的配置信息通知用户。另外，隧道代理会发送配置指令给隧道服务器，隧道服务器根据配置指令进行隧道的建立和维护。经过这些步骤，客户端与隧道服务器之间的 IPv4 封装 IPv6 隧道就建立好了。

10.3.10 隧道配置示例

首先介绍配置隧道的有关命令。各配置命令的语法格式及作用如下。

1. 定义隧道接口的编号

```
Router(config)＃interface tunnel 手动隧道的编号
```

2. 配置隧道接口的 ipv6 地址

```
Router(config)＃ipv6 address ipv6 地址前缀/前缀长度
```

3. 配置隧道源

```
Router(config-if)＃tunnel source 接口|ipv4 地址
```

4. 配置隧道终点

```
Router(config-if)＃tunnel destination ipv4 地址
```

5. 指定隧道的工作模式

```
Router(config-if)#tunnel mode ipv6ip/gre/isatap/6to4
```

例如,命令 tunnel mode ipv6ip 的作用是指定隧道的工作模式为手动配置模式。
下面以图 10-13 所示的网络环境为例,介绍手动配置隧道的具体配置方法。

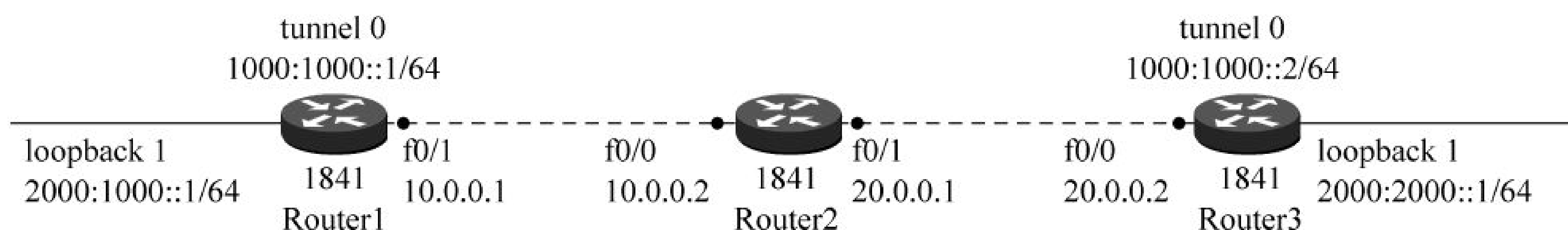


图 10-13 手动配置隧道的网络环境

首先,我们需要建立一条能够传输封装好的 IPv6 报文的 IPv4 隧道,即需要逐一配置这 3 个路由器每个接口的 IPv4 地址、子网掩码和静态路由,具体步骤分别如图 10-14、图 10-15 和图 10-16 所示。

```
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 20.0.0.0 255.0.0.0 10.0.0.2
Router(config)#
```

图 10-14 配置路由器 Router1

```
Router2(config-if)#interface fastethernet 0/0
Router2(config-if)#ip address 10.0.0.2 255.0.0.0
Router2(config-if)#no shutdown
Router2(config-if)#interface fastethernet 0/1
Router2(config-if)#ip address 20.0.0.1 255.0.0.0
Router2(config-if)#no shutdown
Router2(config-if)#
```

图 10-15 配置路由器 Router2

```
Router3(config)#interface fastethernet 0/0
Router3(config-if)#ip address 20.0.0.2 255.0.0.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
Router3(config)#
```

图 10-16 配置路由器 Router3

在图 10-14 中,最后一条命令 ip route 20.0.0.0 255.0.0.0 10.0.0.2 的作用是定义一条从路由器 Router1 到达子网 20.0.0.0 的路由;同理,在图 10-16 中,最后一条命令 ip route 10.0.0.0 255.0.0.0 20.0.0.1 的作用是定义一条从路由器 Router3 到达子网 10.0.0.0 的路由。

至此,IPv4 隧道配置完成,可以用 ping 命令测试 IPv4 网络的连通性,测试结果如图 10-17 所示,表明 IPv4 隧道已经连接正常。

接着,在路由器 Router1 上建立一个环回接口 loopback 1,为其配置 IPv6 地址,并允许使用 IPv6。配置的具体步骤如图 10-18 所示。

```
Router1#ping 20.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.2, timeout is 2 se
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#
```

图 10-17 测试 IPv4 网络的连通性

```
Router1(config)#ipv6 unicast-routing
Router1(config)#interface loopback 1
Router1(config-if)#ipv6 address 2000:1000::1/64
Router1(config-if)#ipv6 enable
Router1(config-if)#
```

图 10-18 配置路由器 Router1 环回接口的 IPv6 地址

同样，在路由器 Router3 上建立一个环回接口 loopback 1，为其配置 IPv6 地址，并允许使用 IPv6。配置的具体步骤如图 10-19 所示。

```
Router3(config)#ipv6 unicast-routing
Router3(config)#interface loopback 1
Router3(config-if)#ipv6 address 2000:2000::1/64
Router3(config-if)#ipv6 enable
Router3(config-if)#
```

图 10-19 配置路由器 Router3 环回接口的 IPv6 地址

此时如果在路由器 Router1 上用 ping 2000:2000::1 命令测试 IPv6 网络的连通性，结果是仍未能 ping 通，原因在于这时仍没有配置好 IPv6 隧道。

接着，分别为路由器 Router1 和路由器 Router2 的环回接口 loopback 1 配置 RIPng 协议，并为隧道接口 tunnel 0 配置 IPv6 地址和 RIPng 协议，如图 10-20 和图 10-21 所示。

```
Router1(config)#ipv6 router rip aa
Router1(config-rtr)#interface loopback 1
Router1(config-if)#ipv6 rip aa enable
Router1(config-if)#interface tunnel 0
Router1(config-if)#ipv6 address 1000:1000::1/64
Router1(config-if)#tunnel source fastethernet 0/1
Router1(config-if)#tunnel destination 20.0.0.2
Router1(config-if)#tunnel mode ipv6ip
Router1(config-if)#ipv6 rip aa enable
Router1(config-if)#ipv6 enable
Router1(config-if)#
```

图 10-20 为路由器 Router1 配置 RIPng 协议

```
Router3(config)#interface loopback 1
Router3(config-if)#ipv6 rip aa enable
Router3(config-if)#interface tunnel 0
Router3(config-if)#ipv6 address 1000:1000::2/64
Router3(config-if)#tunnel source fastethernet 0/0
Router3(config-if)#tunnel destination 10.0.0.1
Router3(config-if)#tunnel mode ipv6ip
Router3(config-if)#ipv6 rip aa enable
Router3(config-if)#ipv6 enable
Router3(config-if)#
```

图 10-21 为路由器 Router3 配置 RIPng 协议

至此，手动隧道配置完成，再次测试 IPv6 隧道的连通性，结果如图 10-22 所示。

```
Router1#ping ipv6 2000:2000::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:2000::1, timeout is
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =

Router1#
```

图 10-22　测试 IPv6 隧道的连通性

此时可以用命令 show ipv6 route 查看路由器的 IPv6 路由表，如图 10-23 所示。

```
Router1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - E
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, C
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   1000:1000::/64 [0/0]
     via ::, Tunnel0
L   1000:1000::1/128 [0/0]
     via ::, Tunnel0
S   2000::/64 [1/0]
     via 1000:1000::2
C   2000:1000::/64 [0/0]
     via ::, Loopback1
L   2000:1000::1/128 [0/0]
     via ::, Loopback1
R   2000:2000::/64 [120/2]
     via FE80::209:7CFF:FED2:975C, Tunnel0
L   FF00::/8 [0/0]
     via ::, Null0
Router1#
```

图 10-23　查看路由器 Router1 的 IPv6 路由表

图 10-23 表明，在路由器 Router1 上，除了直连(C)路由、本地(L)路由和静态(S)路由外，通过 RIPng 协议生成了一条前往子网 2000:2000::/64 的 RIP 动态路由。

此时可以用命令 show ip interface brief 和 show ipv6 interface brief 验证隧道 Tunnel 0 的状态，结果如图 10-24 所示。

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        10.0.0.1        YES manual up                    up
Loopback1              unassigned      YES unset  up                    up
Tunnel0                unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router1#show ipv6 interface brief
FastEthernet0/0            [administratively down/down]
FastEthernet0/1            [up/up]
Loopback1                  [up/up]
    FE80::207:ECFF:FE3E:6DEE
    2000:1000::1
Tunnel0                    [up/up]
    FE80::290:21FF:FEB6:8EB
    1000:1000::1
Vlan1                      [administratively down/down]
Router1#
```

图 10-24　验证隧道接口的状态

从图 10-24 中可以看到，Tunnel 0 在这两种协议中的状态都是 up，表明隧道已经启动，即隧道工作正常。注：由于 Packet Tracer 7.0 模拟器不支持 GRE 隧道、6over4 隧道、6to4 隧道、6RD 隧道、ISATAP 隧道、Teredo 隧道和隧道代理等技术，因此本书对这些隧道技术仅作介绍，而不提供基于 Packet Tracer 7.0 的配置实例。

10.4 协议转换技术

除了以上介绍的双协议栈技术和隧道技术，协议转换技术也可以实现 IPv6 网络和 IPv4 网络之间的连接。协议转换技术通过修改协议报头来转换 IPv4 网络和 IPv6 网络地址，使它们可以互通。协议转换技术下的 IPv4/IPv6 网络互通模型如图 10-25 所示。

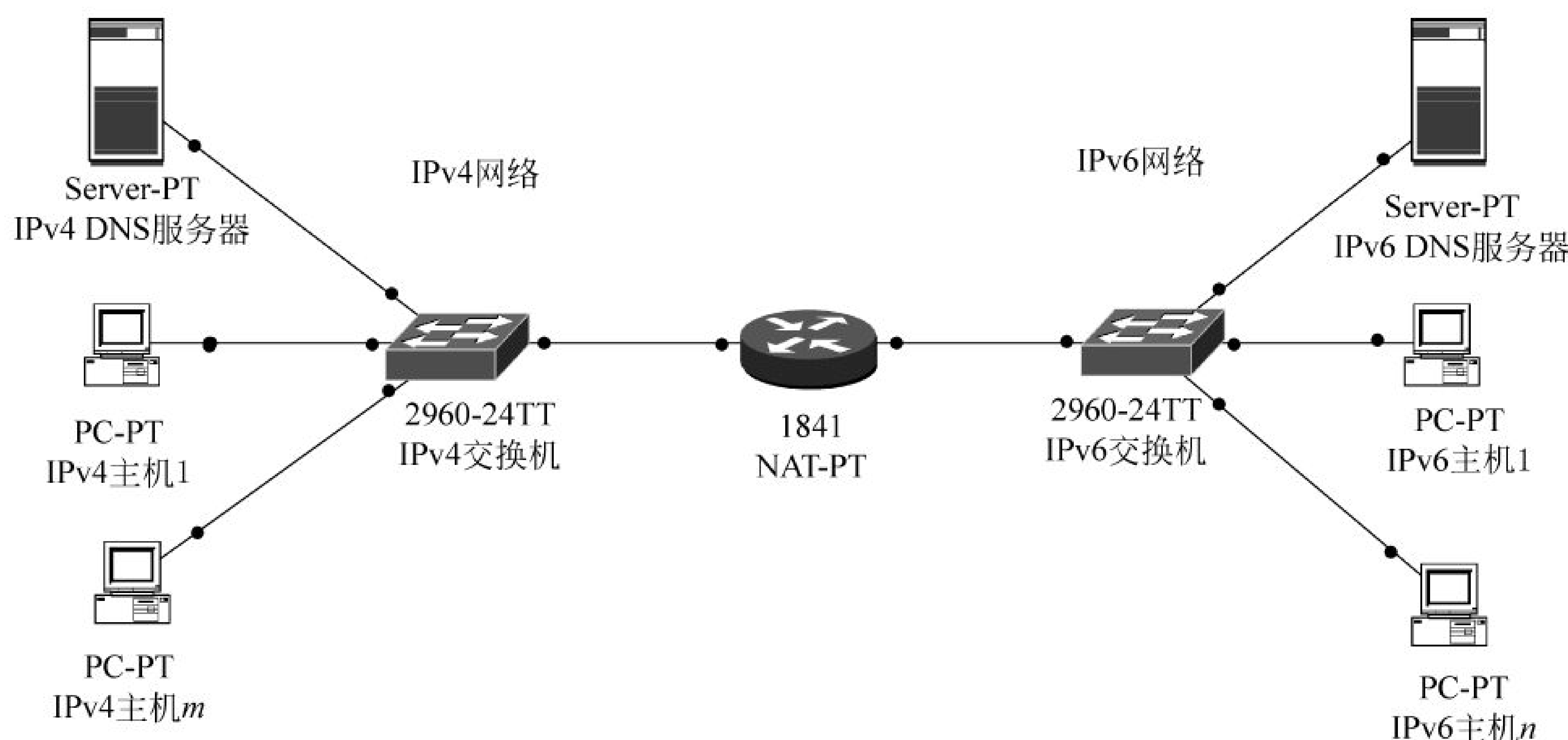


图 10-25 协议转换技术下的 IPv4/IPv6 网络互通模型

协议转换技术通过将 IPv4 结点与 IPv6 结点之间数据包的报头转换为 IPv6 结点与 IPv4 结点之间数据包的报头，为网络通信提供透明的路由。它采用传统的 IPv4 下的 NAT 技术来分配 IPv4 地址，这样就可以用很少的 IPv4 地址构成自己的 IPv4 地址分配池，可以给大量的需要进行地址转换的应用使用协议转换技术服务。常用的协议转换技术分为 NAT-PT 和 NAT64。

10.4.1 NAT-PT

网络地址转换-协议转换(Network Address Translation-Protocol Translation，NAT-PT)是附带协议转换器的网络地址转换器，是一种纯 IPv6 结点和 IPv4 结点间的互通方式，所有包括地址、协议在内的转换工作都由网络设备来完成。

1. NAT-PT 的优缺点

采用 NAT-PT 方式进行过渡的优点是不需要进行 IPv4 结点的升级改造，缺点是 IPv4 结点访问 IPv6 结点的实现方法比较复杂，网络设备进行协议转换、地址转换的处理开销较大，一般在其他互通方式无法使用的情况下使用。

2. NAT-PT 的类型

NAT-PT 机制定义了以下 3 种不同类型的操作：

1）静态 NAT-PT

静态模式提供了一对一的 IPv6 地址和 IPv4 地址的映射。IPv6 单协议网络内的结点要访问的 IPv4 单协议网络内的每个 IPv4 地址都必须在 NAT-PT 设备中设置。每个目的 IPv4 地址在 NAT-PT 设备中被映射为一个具有预定义 NAT-PT 前缀的 IPv6 地址。这种模式中，每个 IPv6 到 IPv4 映射需要一个源 IPv4 地址。静态 NAT-PT 模式与 IPv4 中的静态 NAT 类似。

2）动态 NAT-PT

动态模式也提供了一对一的映射，但是使用一个 IPv4 地址池。池中的源 IPv4 地址数量决定了并发的 IPv6 到 IPv4 转换的最大数目。在 IPv6 网络中，IPv6 单协议网络结点动态地把预定义的 NAT-PT 前缀增加到目的 IPv4 地址。这种模式需要一个 IPv4 地址池来执行动态的地址转换。动态 NAT-PT 模式和 IPv4 中的动态 NAT 类似。

3）NAPT-PT

网络地址端口转换-协议转换（NAPT-PT）模式提供多个有 NAT-PT 前缀的 IPv6 地址和一个源 IPv4 地址间的多对一动态映射。这种转换同时在第三层（IPv4/IPv6）和上层（TCP/UDP）进行。NAPT-PT 和 IPv4 中的 PAT 转换类似。

10.4.2 NAT64

在过渡期间，IPv4 和 IPv6 共存的过程中面临的一个主要问题是 IPv6 与 IPv4 之间如何互通。由于二者的不兼容性，因此无法实现两种不兼容网络之间的互访。为了解决这个难题，IETF 在早期设计了 NAT-PT 的解决方案——RFC 2766，NAT-PT 通过 IPv6 与 IPv4 的网络地址与协议转换实现了 IPv6 网络与 IPv4 网络的双向互访。但 NAT-PT 在实际网络应用中面临各种缺陷，IETF 不再推荐使用 NAT-PT，因此 NAT-PT 已被 RFC 4966 淘汰。

为了解决 NAT-PT 中的各种缺陷，同时实现 IPv6 与 IPv4 之间的网络地址与协议转换技术，IETF 重新设计了一项新的解决方案——NAT64 ＋ DNS64 技术。

NAT64 的工作原理如图 10-26 所示。

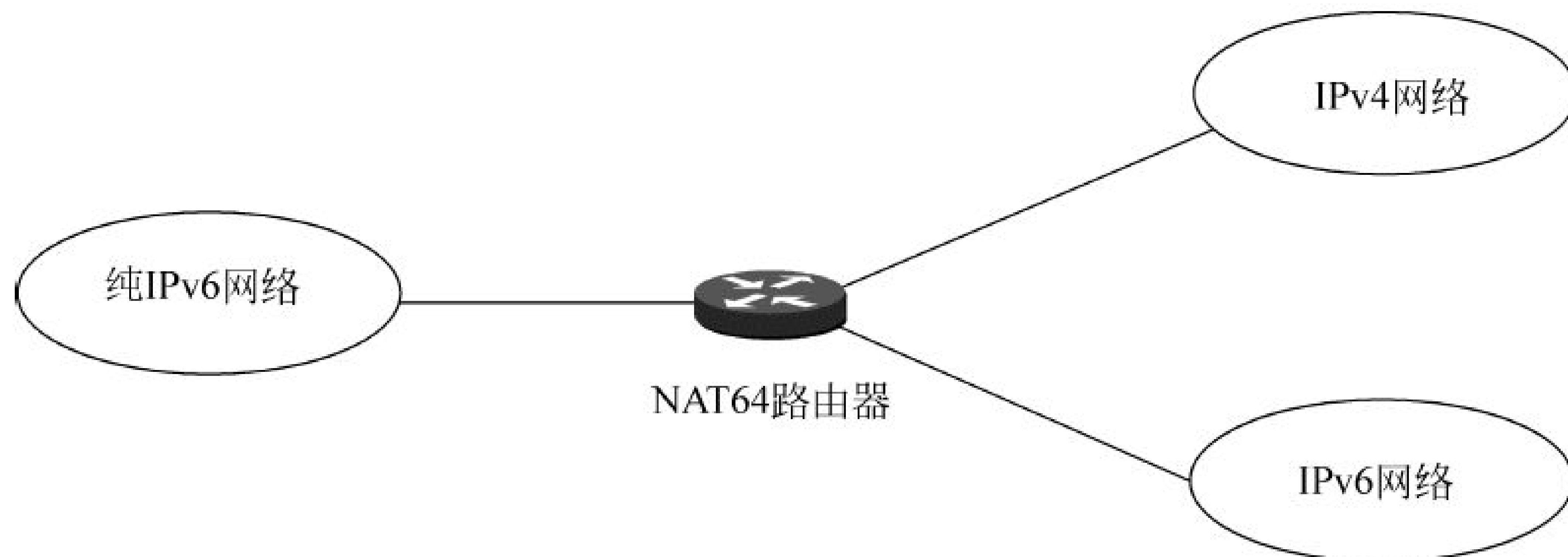


图 10-26 NAT64 的工作原理

NAT64 的主要目的是允许纯 IPv6 客户端向纯 IPv4 服务器发起通信过程。利用静态或手动式绑定机制，NAT64 也允许纯 IPv4 客户端向纯 IPv6 服务器发起通信。

NAT64 是一种有状态的网络地址与协议转换技术，一般只支持通过 IPv6 网络侧用户发起连接访问 IPv4 侧网络资源。但 NAT64 也支持通过手工配置静态映射关系，实现 IPv4 网络主动发起连接访问 IPv6 网络。NAT64 可实现 TCP、UDP、ICMP 下的 IPv6 与 IPv4 网络地址和协议转换。域名解析服务器 DNS64 则主要是配合 NAT64 工作。

NAT64 是一种 IPv6 到 IPv4 的转换技术，主要考虑过渡初期 IPv6 终端对 IPv4 资源的访问，不涉及 IPv4 访问 IPv6 资源的情况。NAT64 可实现 TCP、UDP、ICMP 下的 IPv6 与 IPv4 网络地址和协议转换。

NAT64 要正常工作，通常还需要配套 DNS64。DNS64 可以将 DNS 查询信息中的 A 记录(IPv4 地址)合成到 AAAA 记录(IPv6 地址)中，返回合成的 AAAA 记录用户给 IPv6 侧用户。

NAT64 包括 3 类组件：NAT64 前缀、DNS64 服务器和 NAT64 路由器。

1. NAT64 前缀

为了通过纯 IPv6 网络传输数据包转化后的 IPv4 地址一起使用的任何/32、/40、/48、/56、/64 或/96 前缀，NAT64 前缀可以是特定网络前缀(Network Specific Prefix，NSP)或周知前缀(Well-Known Prefix，WKP)。NSP 是由组织机构自行分配的前缀，通常来自组织机构自有 IPv6 前缀的子网。用于 NAT64 的 WKP 地址是 64:FF9B::/96。如果没有指定或配置 NSP，那么 NAT64 就将 WKP 附加到转化后的 IPv4 地址上。NAT64 前缀也称为 Pref64::/n。

2. DNS64 服务器

DNS64 服务器不但为 IPv6 AAAA 记录完成普通的 DNS 服务器功能，而且还要在 AAAA 记录不可用时试图定位 IPv4 A 记录。定位了 IPv4 A 记录之后，DNS64 会利用 NAT 前缀将 IPv4 A 记录转换为 IPv6 AAAA 记录，使得纯 IPv6 主机认为其可以通过 IPv6 与纯 IPv4 服务器进行通信。

3. NAT64 路由器

NAT64 路由器将 NAT64 前缀宣告到纯 IPv6 网络中，并在纯 IPv6 网络与纯 IPv4 网络之间执行转换操作。

DNS64 将 IPv4 A 记录合成为 IPv6 AAAA 记录的工作原理如图 10-27 所示。

DNS64 服务器收到 www.example.com 的 IPv4 A 记录后，将这个 IPv4 地址转化为十六进制 0A0A:0A0A，然后将前缀 2001:DB8:CAFE:AAAA::/96 放到 0A0A:0A0A 之前，就可得到 DNS64 合成后的 www.example.com 的 AAAA 记录 2001:DB8:CAFE:AAAA::0A0A:0A0A。这个地址会被用作访问 www.example.com 服务器的 IPv6 地址。

10.4.3 NAT64 配置示例

RFC 6146 定义了从 IPv6 客户端到 IPv4 服务器的状态化 NAT64 网络地址和协议转换机制。与 IPv4 使用的状态化 NAT 相似，状态化 NAT64 在执行协议转换的同时会创建或修改 IPv6 与 IPv4 之间的绑定关系。

NAT64 相关配置命令的语法格式及其作用说明如下。

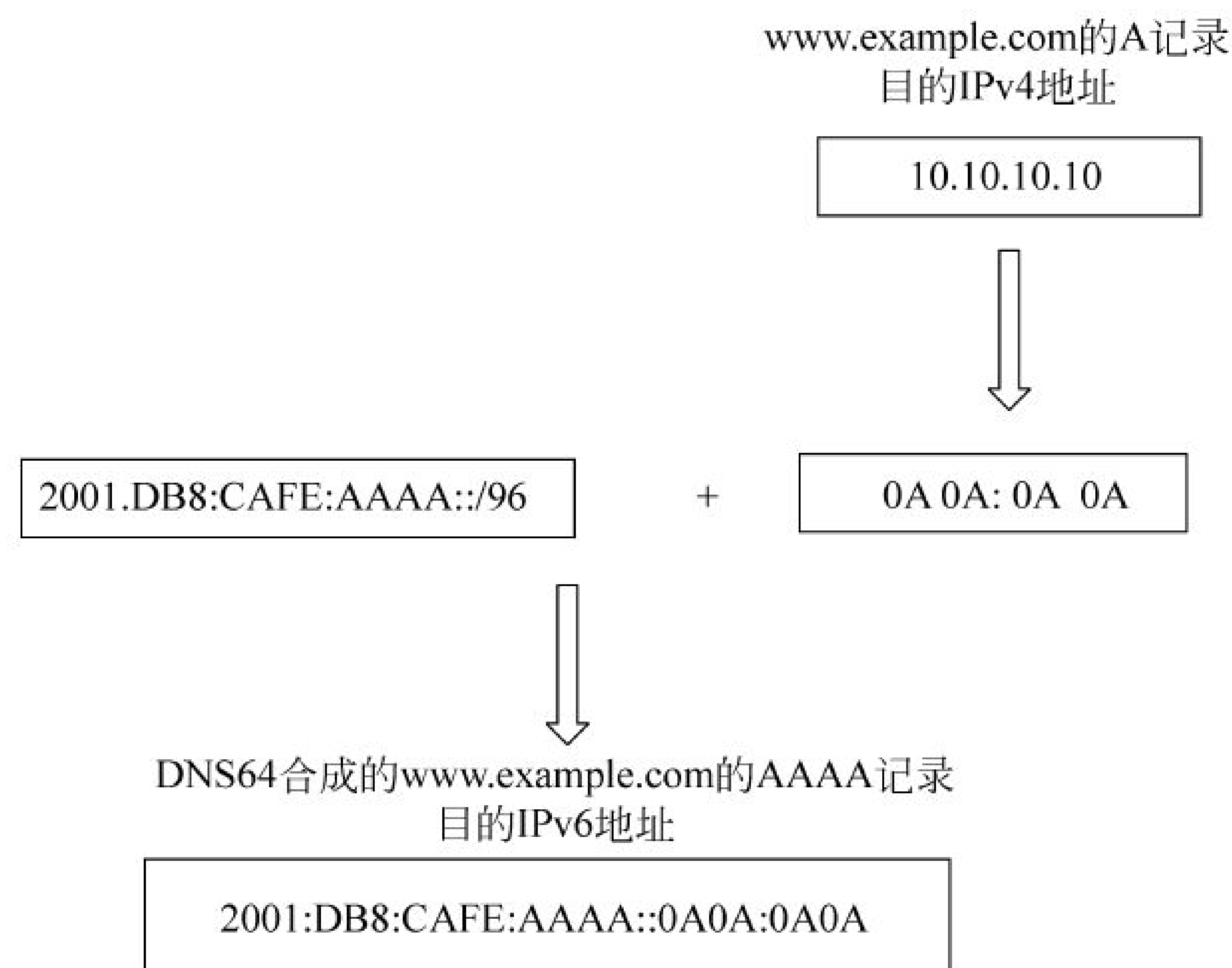


图 10-27　DNS64 将 IPv4 记录合成为 IPv6AAAA 记录的工作原理

1. 指定接口类型和接口号，并进入接口配置模式

```
Router(config)# interface 接口类型 接口号
```

2. 为当前接口配置 IPv4 地址和子网掩码

```
Router(config-if)# ip address ipv4 地址 子网掩码
```

3. 为当前接口配置 IPv6 地址和前缀长度

```
Router(config-if)# ipv6 address ipv6 地址/前缀长度
```

4. 在当前接口上启用 NAT64 转换功能

```
Router(config-if)# nat64 enable
```

5. 为状态化 NAT64 定义 IPv6 前缀和前缀长度

```
Router(config)# nat64 prefix stateful ipv6 前缀和前缀长度
```

6. 启用 NAT64 IPv4 配置

```
Router(config)# nat64 v4 pool 地址池名字 起始地址 结束地址
```

7. 将 IPv6 源地址转换为 IPv4 源地址，并将 IPv4 目的地址转换为 IPv6 目的地址

```
Router(config)# nat64 v6v4 list ACL 表名 pool NAT64 地址池名字 [overload]
```

其中，参数 overload 是可选项，用于启用 NAT64 超量地址转换功能。

8. 定义 IPv6 ACL 并进入 IPv6 访问控制列表配置模式

```
Router(config)# ipv6 access-list IPv6 访问控制列表名字
```

9. 指定将要转换的 IPv6 地址和前缀长度

```
Router(config)# ipv6 permit ipv6 地址/前缀长度
```

下面以图 10-28 为例，介绍 NAT64 的配置方法。具体的配置步骤如图 10-29 所示。



图 10-28 配置 NAT64 的网络环境

```
1  Router(config-if)#interface fastethernet 0/0
2  Router(config-if)#description Connected to IPv6 Network
3  Router(config-if)#ipv6 address 2001:DB8:CAFE:1::101/64
4  Router(config-if)#nat64 enable
5  Router(config-if)#exit
6  Router(config)#interface fastethernet 0/1
7  Router(config-if)#description Connected to IPv4 Network
8  Router(config-if)#ip address 192.168.99.1 255.255.255.0
9  Router(config-if)#no shutdown
10 Router(config-if)#nat64 enable
11 Router(config-if)#exit
12 Router(config)#nat64 prefix stateful 2001:DB8:CAFE:AAAA::/96
13 Router(config)#nat64 v4 pool pool1 192.168.99.2 192.168.99.10
14 Router(config)#nat64 v6v4 list mylist pool1 overload
15 Router(config)#ipv6 access-list mylist
16 Router(config-ipv6-acl)#permit ipv6 2001:DB8:CAFE::/48 any
```

图 10-29 配置 NAT64 路由器

在图 10-29 中，第 1 行命令的作用是指定配置接口为 fastethernet 0/0，并进入接口配置模式。

第 2 行命令的作用是说明这是一个纯 IPv6 网络。

第 3 行命令的作用是为接口配置 IPv6 全局单播可路由地址。

第 4 行命令的作用是在当前接口上启用无状态 NAT64 协议转换功能。

第 5 行命令的作用是退出，回到全局配置模式。

第 6 行命令的作用是指定配置接口为 fastethernet 0/1，并进入接口配置模式。

第 7 行命令的作用是说明这是一个纯 IPv4 网络。

第 8 行命令的作用是为接口配置 IPv4 地址和子网掩码。

第 9 行命令的作用是激活接口。

第 10 行命令的作用是在当前接口上启用无状态 NAT64 协议转换功能。

第 11 行命令的作用是退出，回到全局配置模式。

第 12 行命令的作用是启用 NAT64 的 IPv6-to-IPv4 地址映射，将使用 NAT64 前缀地址 2001:DB8:CAFE:AAAA::/96，并附加一个 IPv4 地址。

第 13 行命令的作用是定义 NAT64 IPv4 地址池，这些地址都是用于 NAT64 转换的 IPv4 地址。

第 14 行命令的作用是将 IPv4 源地址动态转换为 IPv6 源地址，并将 IPv6 目的地址转换为 IPv4 目的地址。参数 overload 的作用是启用 NAT64 超量地址转换功能。

第 15 行命令的作用是定义一个 IPv6 访问控制列表，并进入 IPv6 访问控制列表配置模式。

第 16 行命令的作用是指定将要转换的 IPv6 地址和前缀长度。

10.5 本章总结

虽然 IPv6 网络取代 IPv4 网络是一种必然的趋势，但是实现 IPv6 技术的全面应用仍然需要相当长的一段时间。也就是说，IPv4 是逐步过渡到 IPv6 的。过渡技术重点解决如何在 IPv4 网络环境里实现与 IPv6 网络的互操作及平滑过渡问题。

目前，从 IPv4 过渡到 IPv6 的技术主要分为 3 大类：双协议栈技术、隧道技术和 IPv4/IPv6 协议转换技术。

双协议栈技术是指在网络结点上同时运行 IPv4 和 IPv6 两种协议，从而在 IP 网络中形成逻辑上相互独立的两张网络：IPv4 网络和 IPv6 网络。网络中的结点同时支持 IPv4 和 IPv6 协议栈，源结点根据目的结点的不同选用不同的协议栈，而网络设备根据报文的协议类型选择不同的协议栈进行处理和转发。

隧道(Tunneling)技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将其他协议的数据帧或包重新封装，然后通过隧道发送。新的帧头提供路由信息，以便通过互联网传递被封装的负载数据。

隧道的类型有多种，根据隧道协议的不同来分，可以将隧道分为 IPv4 over IPv6 隧道和 IPv6 over IPv4 隧道；根据隧道终点地址的获得方式来分，可以将隧道分为配置型隧道(如手动配置隧道、GRE 隧道)和自动配置的兼容隧道(如 6over4、6to4、6RD、ISATAP、Teredo、隧道代理等)。

手动配置隧道(Manually Configured Tunnel，RFC 2893)是通过 IPv4 骨干网连接的两个 IPv6 域的一条永久链路，这条永久链路用于两个边缘路由器或终端系统与边缘路由器之间定期安全通信的稳定连接。手动配置隧道适用于两台边缘路由器或者边缘路由器和主机之间对安全性要求比较高并且比较固定的连接上。

GRE 隧道报文首先在 IPv6 首部添加一个 GRE 首部，再把整个数据包作为 IPv4 报文的有效数据部分封装在 IPv4 报文中，而 IPv4 报文的源地址和目的地址都是在 GRE 隧道接口配置中手动指定的。手动的 GRE 隧道并不适用于大量部署，一般只用于隧道端点相对固定的场景中。

自动配置的兼容隧道需要站点采用与 IPv4 兼容的 IPv6 地址(IPv4 Compatible IPv6 address)，即 0::a.b.c.d/96，其中，a.b.c.d 是 IPv4 地址。这些站点之间必须有可用的 IPv4 连接，每个采用这种机制的主机都需要有一个全球唯一的 IPv4 地址。

RFC 2529 定义的 IPv4 组播隧道(6over4)是一种 IPv4 组播隧道机制，通过将 IPv6 数据包封装在 IPv4 中的方式连接互相分离的 IPv6 主机。6over4 主机的 IPv6 地址由 64 位的单播地址前缀和规定格式的 64 位接口标识符：AABB:CCDD 组成，其中 AABB:CCDD 是其 IPv4 地址 a.b.c.d 的十六进制表示。

RFC 3056 定义的 6to4 也是一种自动构造隧道的机制，这种机制要求站点采用特殊的 IPv6 地址，即 2002:a.b.c.d::/48，其中，a.b.c.d 是相应的 IPv4 地址。这种特殊地址是自动从站点的 IPv4 地址派生出来的。所以，每个采用 6to4 机制的结点必须具有一个全球唯

一的 IPv4 地址，这种地址分配方法可以使得其他域的边界路由器自动地区分隧道接收端点是否在本域内。

6RD 是 IPv6 快速部署(IPv6 Rapid Deployment)的简称，其对应的标准为 RFC 5569。6RD 隧道技术是由法国运营商 FREE 提出的。FREE 在提出该方案的短短 5 周内就已经为超过 150 万户用户提供了 IPv6 服务。6RD 是在 6to4 基础上发展起来的一种 IPv6 网络过渡技术方案。

站内自动隧道寻址协议(ISATAP)是一种地址分配和主机到主机、主机到路由器、路由器到主机的自动隧道技术，它为 IPv6 主机之间提供了跨越 IPv4 内部网络的单播 IPv6 连通性。ISATAP 一般用于 IPv4 网络中的 IPv6/IPv4 结点间的通信。

ISATAP 使用本地管理的接口标识符::0:5EFE:w.x.y.z，其中::0:5EFE 部分是由 Internet 号码分配中心(IANA)分配的机构单元标识符(00-00-5E)和表示内嵌的 IPv4 地址类型的类型号(FE)组合而成的。w.x.y.z 部分是任意的单播 IPv4 地址，既可以是私有地址，也可以是公共地址。

Teredo 隧道是一种 IPv6 over UDP 隧道。因为传统的 NAT 技术不能支持 IPv6 over IPv4 数据包的穿越，所以，为了解决这个问题，采用把 IPv6 数据包封装在 UDP 载荷中的方式穿过 NAT。

隧道代理的主要目的是简化隧道的配置，提供自动的配置手段。从这个意义上说，隧道代理可以看作是一个虚拟的 IPv6 ISP，通过 Web 方式为用户分配 IPv6 地址，建立隧道，以提供和其他 IPv6 站点的通信。隧道代理的特点是灵活、可操作性强，针对不同用户可提供不同的隧道配置。

协议转换技术通过将 IPv4 结点与 IPv6 结点之间数据包的报头转换为 IPv6 结点与 IPv4 结点之间数据包的报头，为网络通信提供透明的路由。它采用传统的 IPv4 下的 NAT 技术来分配 IPv4 地址，这样就可以用很少的 IPv4 地址构成自己的 IPv4 地址分配池，可以给大量的需要进行地址转换的应用使用协议转换技术服务。常用的协议转换技术分为 NAT-PT 和 NAT64。

网络地址转换-协议转换(Network Address Translation-Protocol Translation，NAT-PT)是附带协议转换器的网络地址转换器，是一种纯 IPv6 结点和 IPv4 结点间的互通方式，所有包括地址、协议在内的转换工作都由网络设备来完成。

NAT64 是一种有状态的网络地址与协议转换技术，一般只支持通过 IPv6 网络侧用户发起连接访问 IPv4 侧网络资源。但 NAT64 也支持通过手工配置静态映射关系，实现 IPv4 网络主动发起连接访问 IPv6 网络。NAT64 可实现 TCP、UDP、ICMP 下的 IPv6 与 IPv4 网络地址和协议转换。DNS64 则主要是配合 NAT64 工作，将 DNS 查询信息中的 A 记录(IPv4 地址)合成到 AAAA 记录(IPv6 地址)中，返回合成的 AAAA 记录用户给 IPv6 侧用户。

复习思考题

1. 目前比较成熟的从 IPv4 向 IPv6 过渡的 3 种技术是什么?
2. 双协议栈技术的工作原理是什么?
3. 实现双协议栈的关键技术是什么?

4. ICMPv6 是一种什么协议？其主要功能是什么？
5. 邻居发现协议是一种什么协议？其主要功能是什么？
6. 什么是域名系统？其主要功能是什么？
7. 如何实现 DNS 服务器的冗余？
8. 请说明手动配置隧道的工作原理。
9. 请说明 GRE 隧道的工作原理。
10. 请说明自动配置 IPv4 兼容隧道的工作原理。
11. 请说明 6over4 隧道的工作原理。
12. 请说明 6to4 隧道的工作原理。
13. 请说明 6RD 隧道的工作原理。
14. 请说明 ISATAP 隧道的工作原理。
15. 请说明 Teredo 隧道的工作原理。
16. 请说明隧道代理的工作原理。
17. 什么是协议转换技术？
18. 什么是 NAT64？
19. 实训操作题 1：请按照图 10-30 所示的网络环境配置 IPv6 手动隧道，使路由器 Router1 的环回接口 loopback 1 与路由器 Router2 的环回接口 loopback 1 能通过手动隧道连通。

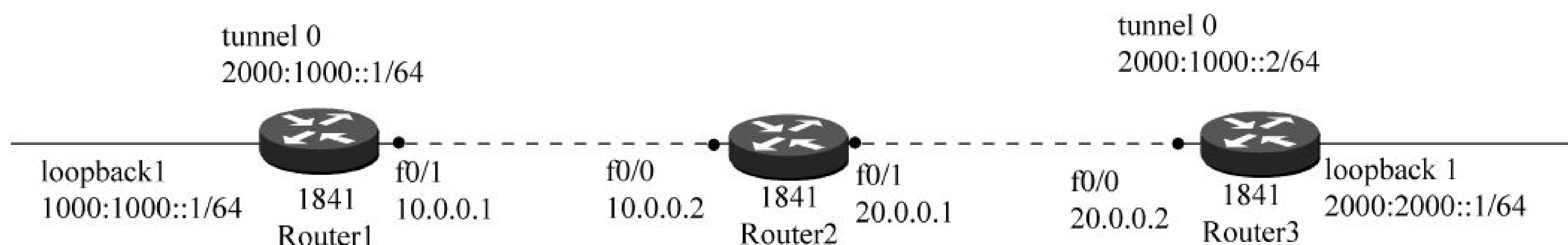


图 10-30　IPv6 手动隧道的网络配置环境

20. 实训操作题 2：请按照图 10-31 所示的网络环境配置 NAT64，使 IPv6 地址为 1001::100/64 的主机 PC1 能够访问 IPv4 地址为 10.10.10.8 的 Web 服务器。

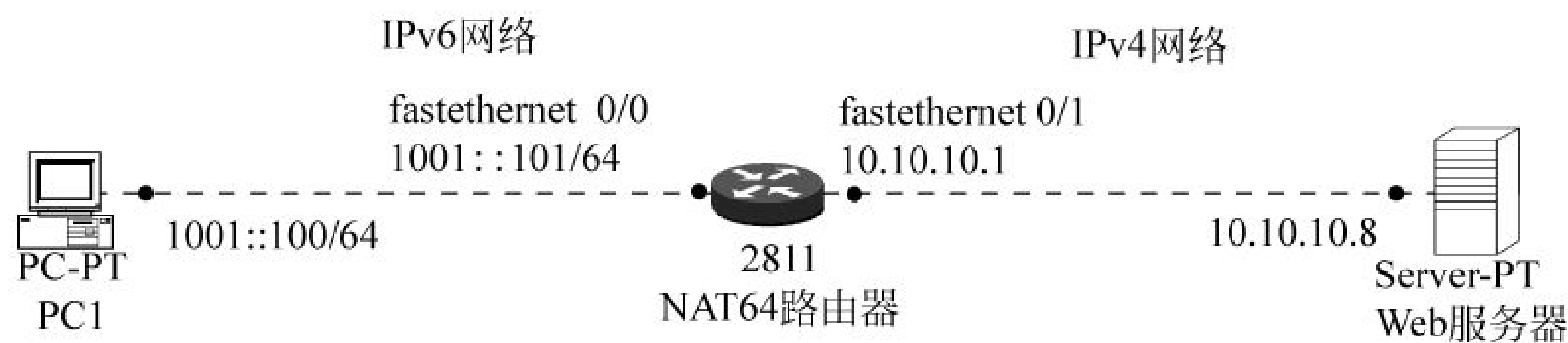


图 10-31　配置 NAT64 的网络环境

附　　录

附录 A 思科 Packet Tracer 7.0 使用简介

APPENDIX A

Packet Tracer 是 Cisco 公司推出的一款功能强大的网络设备(如路由器和交换机等)模拟软件,目前最新的版本是 7.0 版,主要实现 Cisco 设备的图形界面的模拟功能。这款软件通过建立虚拟的网络环境,能让用户通过对网络环境中的路由器、交换机和计算机主机等网络设备进行模拟,能够直观地演示网络设备的运行情况,使用非常方便。Packet Tracer 7.0 支持学生和教师建立仿真、虚拟活动网络模型,通过仿真技术对现实的网络设备进行仿真,让用户可以在虚拟的环境下建立网络拓扑结构图,支持 JavaScript 和 CSS,支持多种路由器、交换机和服务器,为学习网络技术课程的初学者设计和配置网络、排除网络故障提供了简单、易用的模拟环境。

A.1 Packet Tracer 7.0 安装方法

Packet Tracer 7.0 的安装程序分为两个版本,即 32 位版本和 64 位版本。首先,从网络上下载并解压文件,用杀毒软件扫描确认文件安全后,找到安装程序 PacketTracer70_32bit_setup(32 位)或 PacketTracer70_64bit_setup(64 位),双击即可开始安装,显示安装向导页面,如图 A-1 所示。

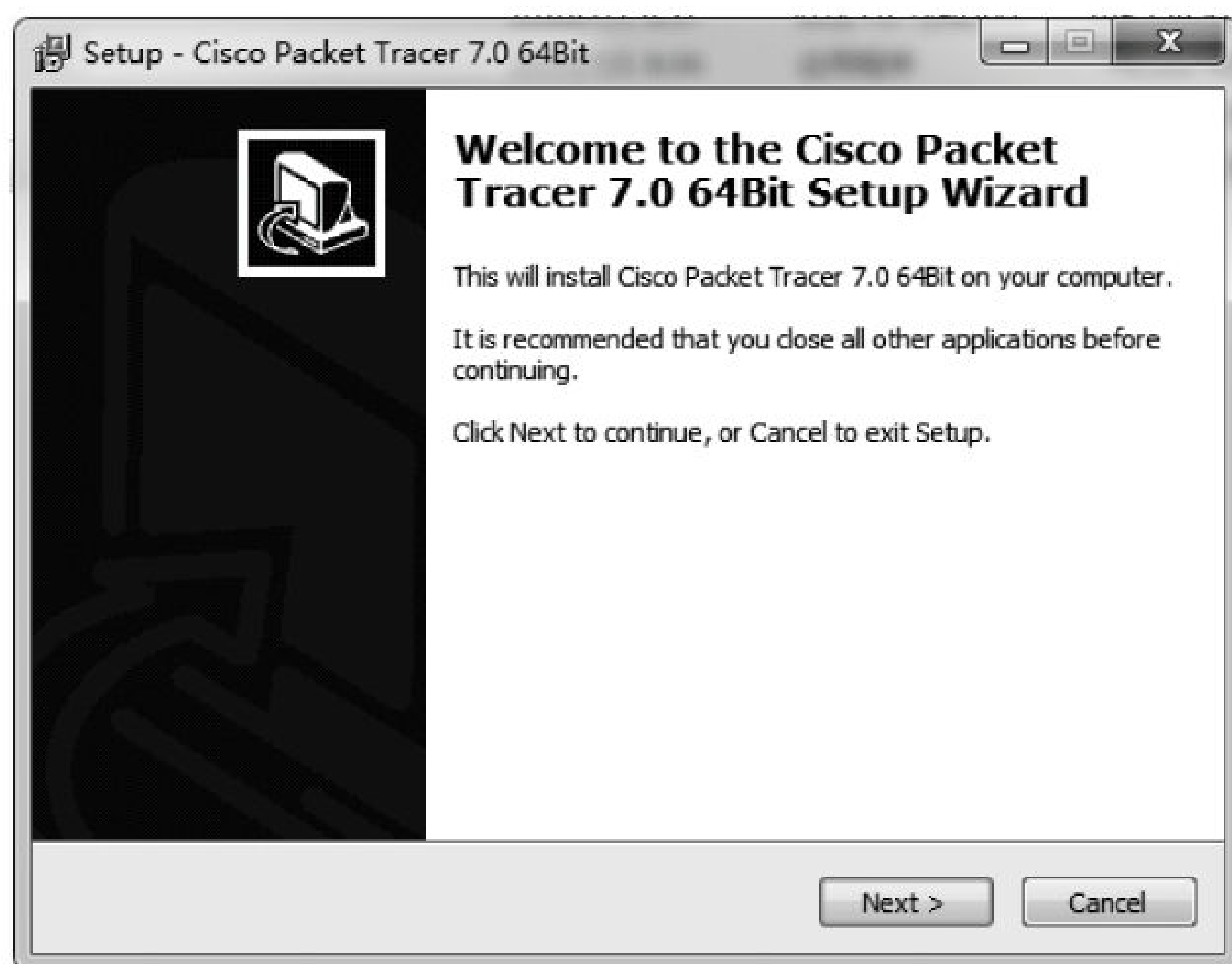


图 A-1 Packet Tracer 7.0 的安装向导

单击 Next 按钮，出现如图 A-2 所示的软件授权协议窗口。

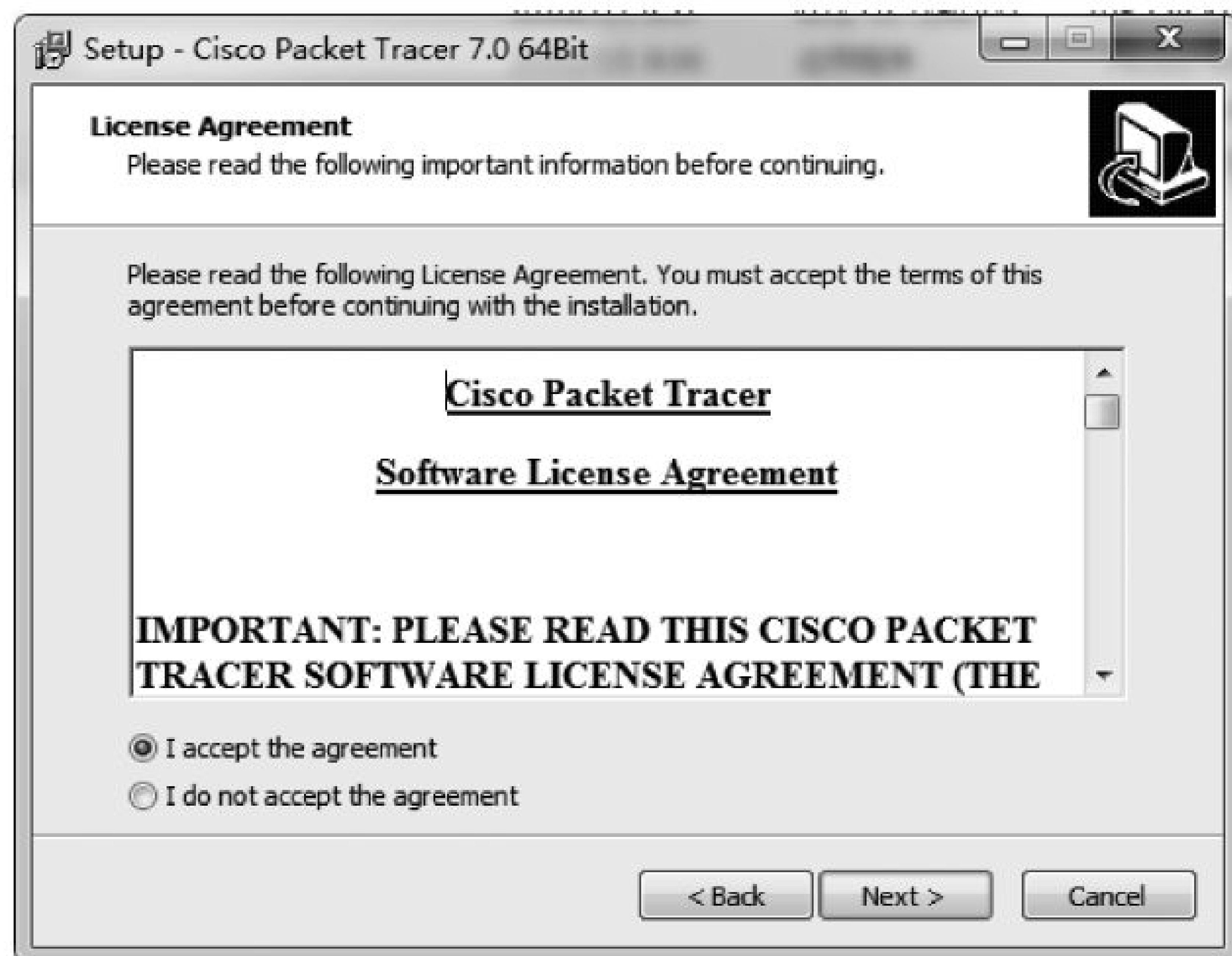


图 A-2　Packet Tracer 7.0 的软件安装协议

选中 I accept the agreement(同意协议)，单击 Next 按钮出现如图 A-3 所示的窗口。

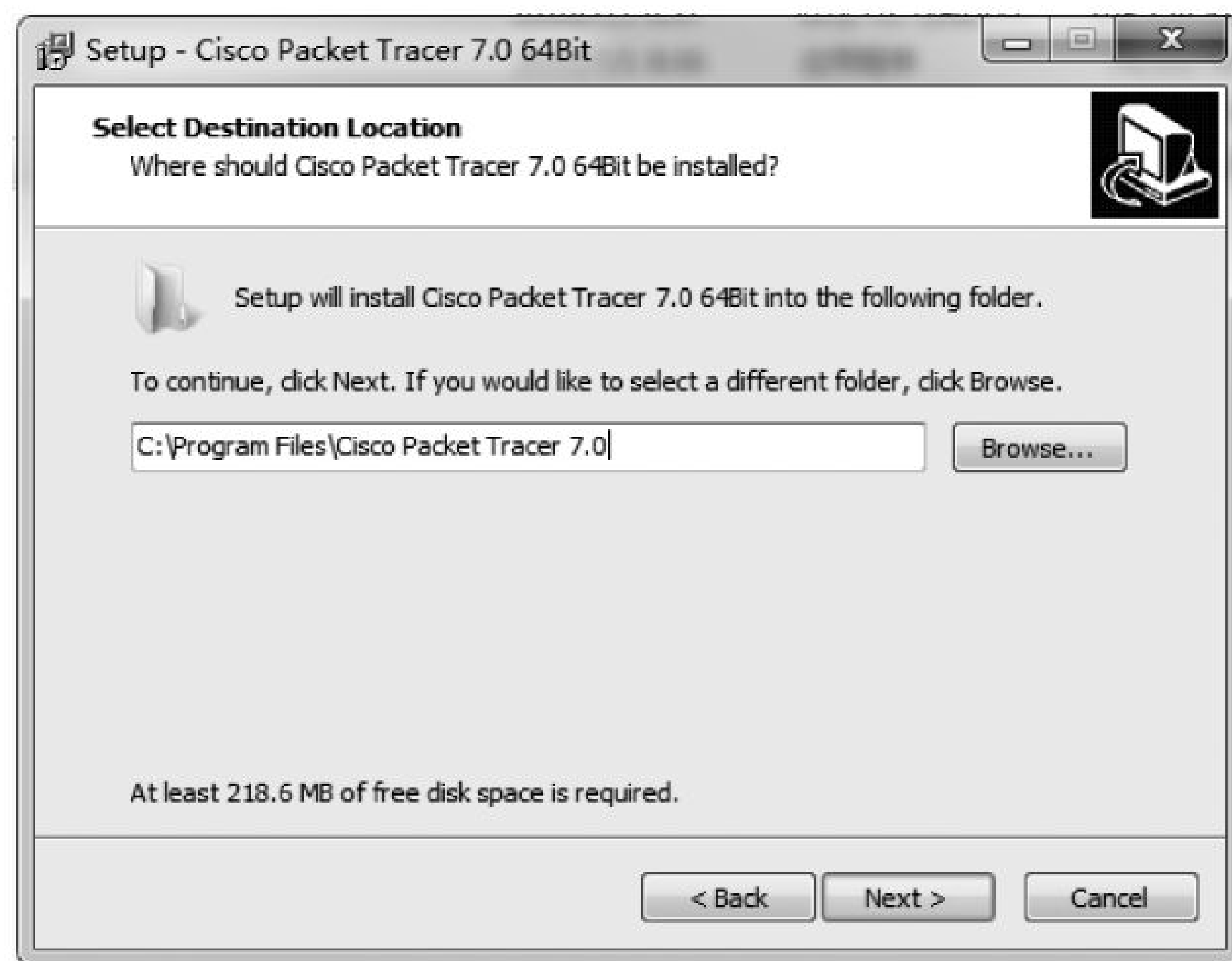


图 A-3　修改 Packet Tracer 7.0 软件的安装位置

单击 Browse 按钮可修改 Packet Tracer 7.0 的安装位置，单击 Next 按钮会出现如图 A-4 所示的页面，此时可以修改开始菜单文件夹的名称，单击 Next 按钮出现如图 A-5 所示的页面。

在图 11-5 中勾选 Create a desktop icon 建立桌面图标，然后单击 Next 按钮出现如图 A-6 所示的页面。接着，单击 Install 按钮开始安装 Packet Tracer 7.0，安装过程如图 A-7 所示。

最后出现如图 A-8 所示的页面，表明 Packet Tracer 7.0 已经安装完成。

Packet Tracer 7.0 安装完成后，计算机屏幕中将会出现如图 A-9 所示的页面。

图 A-9 出现的信息是提醒用户关闭所有浏览器或重新启动计算机。此时，请按要求关闭所有浏览器窗口或重新启动计算机，然后就可以运行 Packet Tracer 7.0 了。

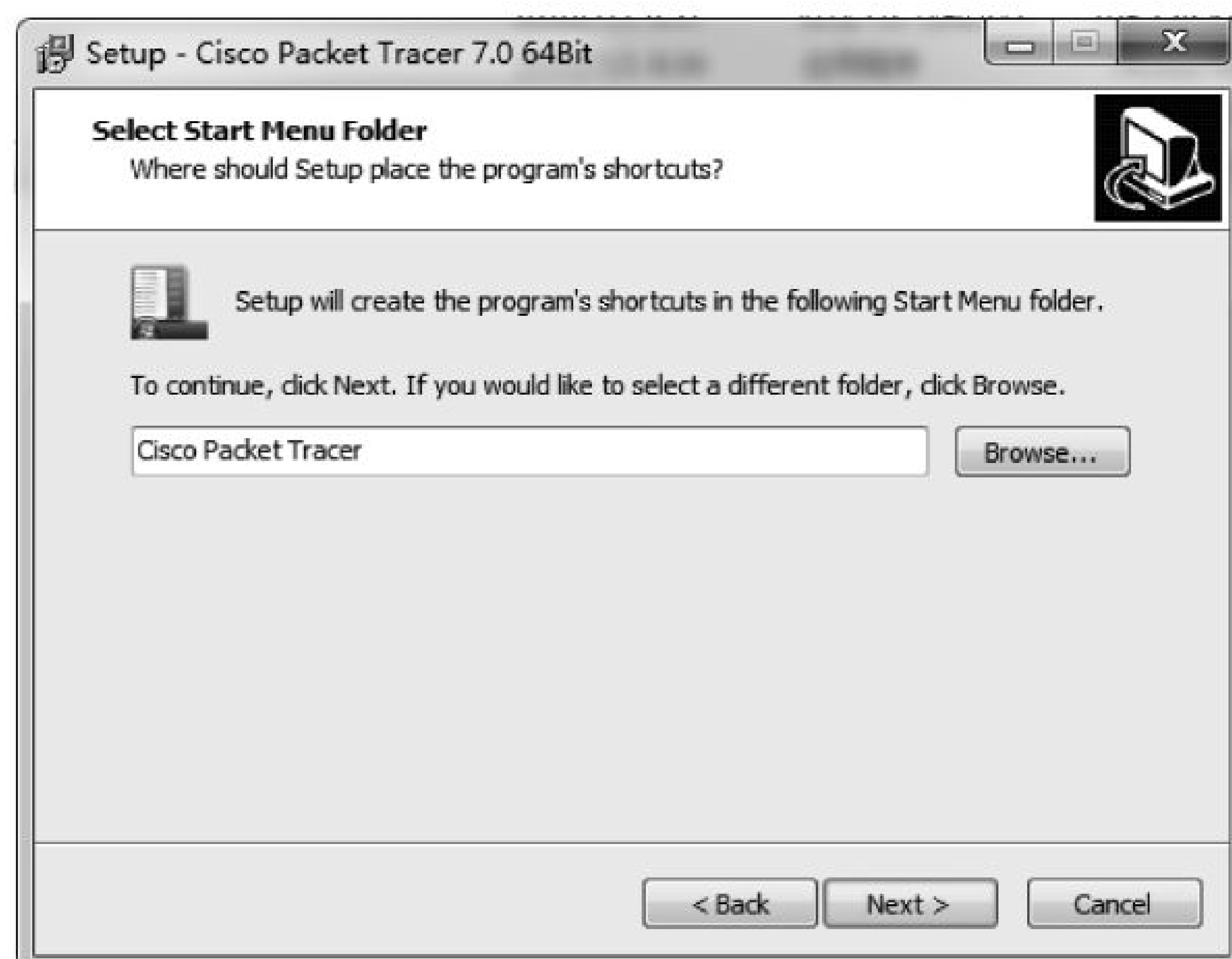


图 A-4 修改开始菜单文件夹的名称

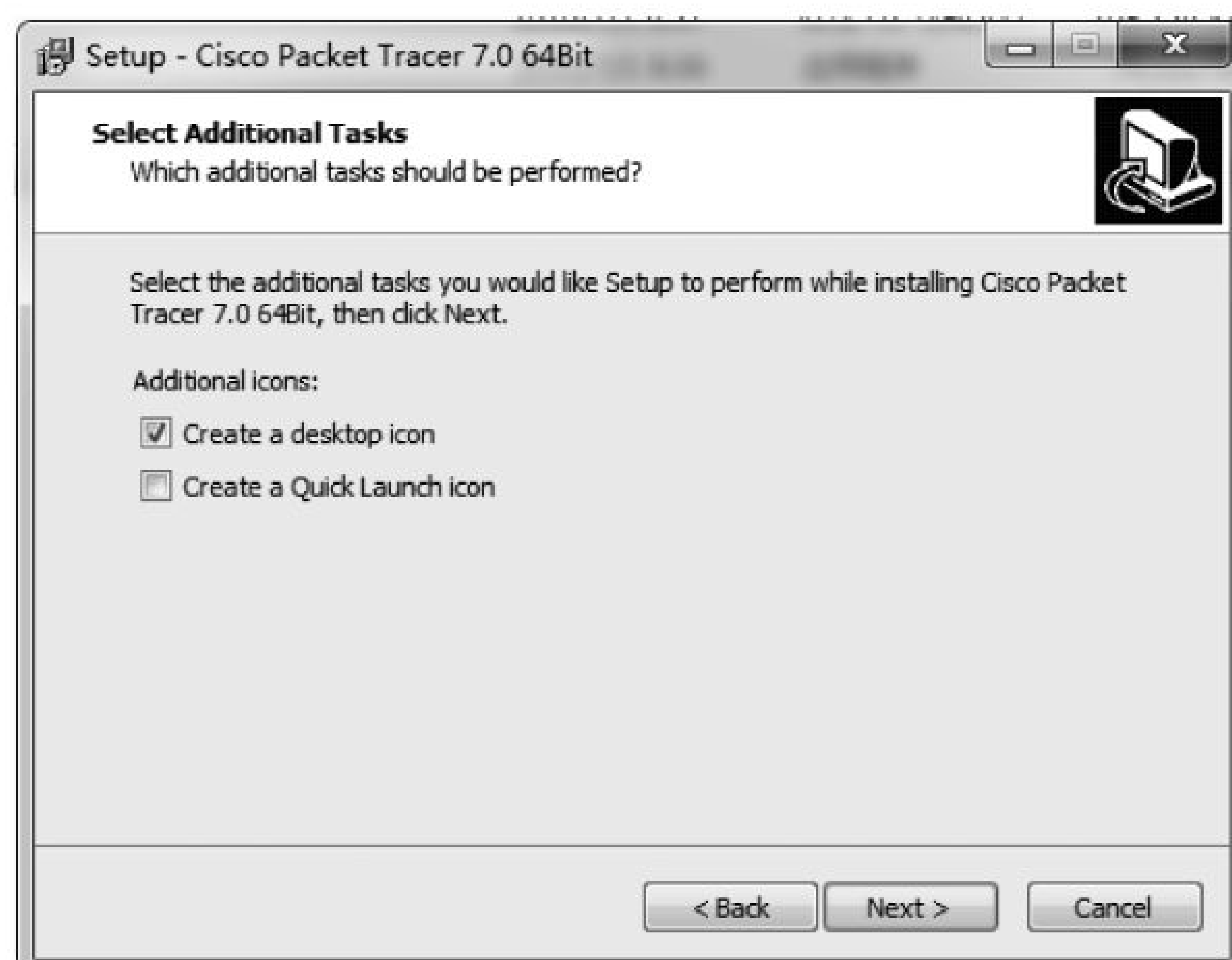


图 A-5 建立启动 Packet Tracer 7.0 的桌面图标

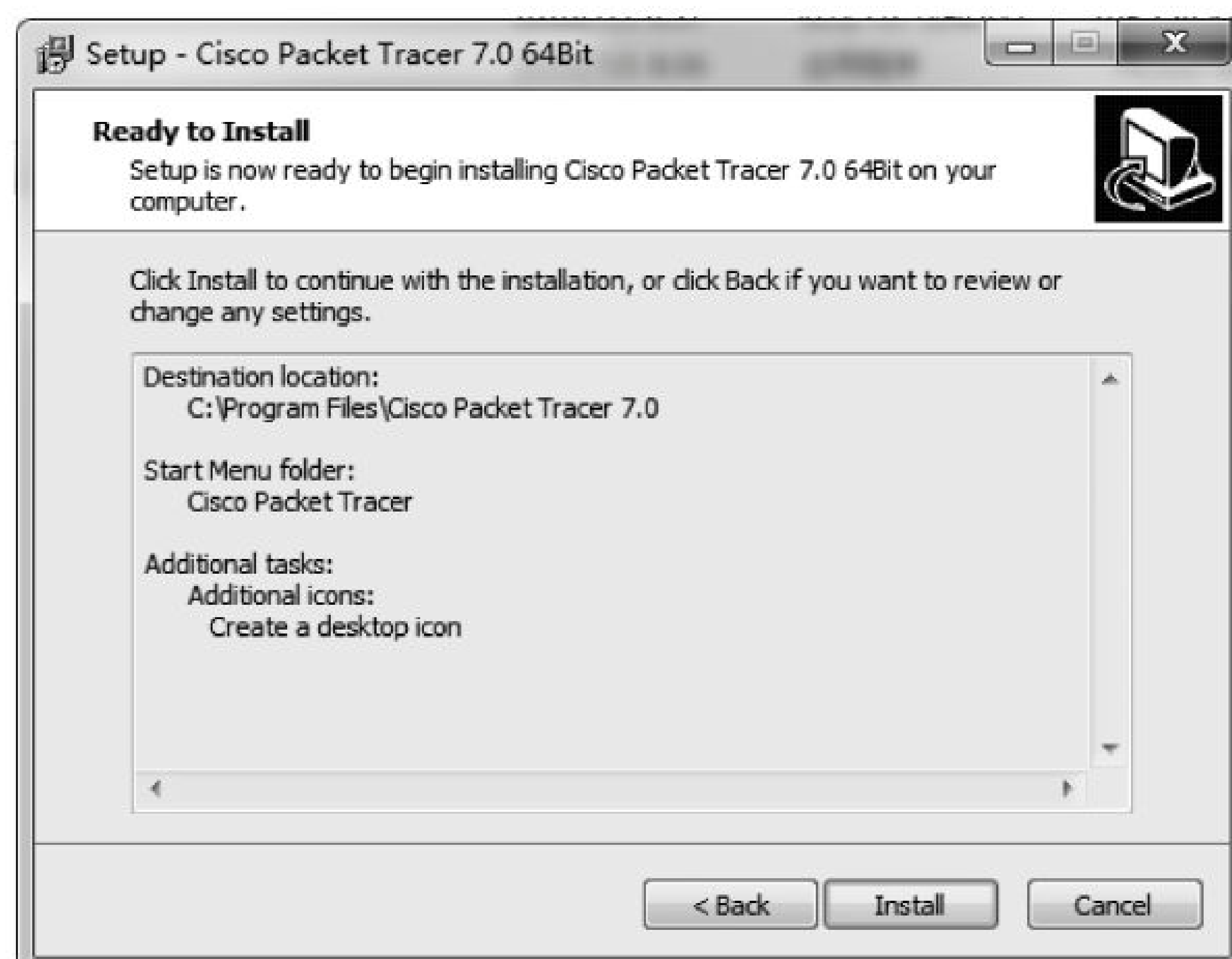


图 A-6 准备安装 Packet Tracer 7.0

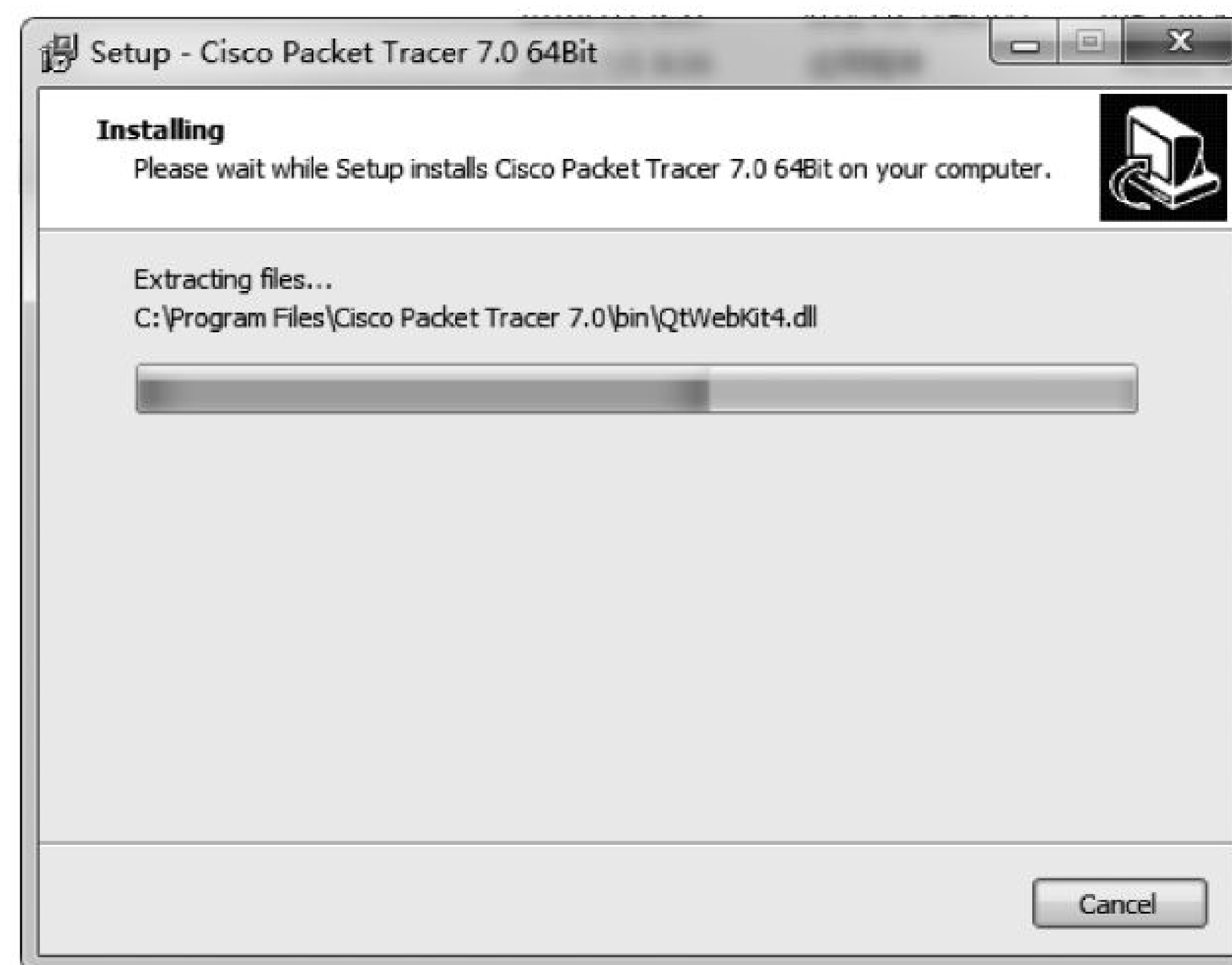


图 A-7　Packet Tracer 7.0 的安装过程

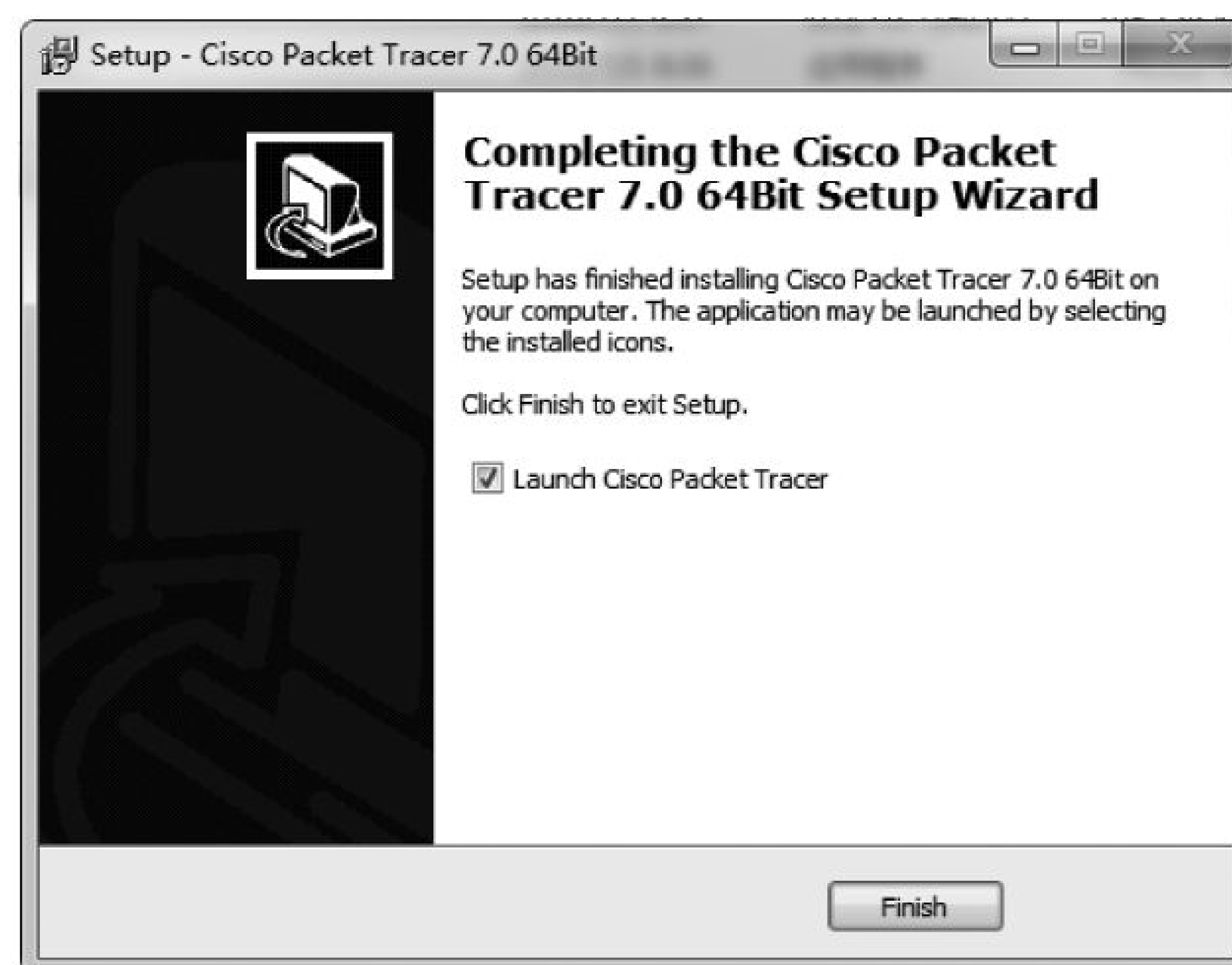


图 A-8　Packet Tracer 7.0 安装完成的页面

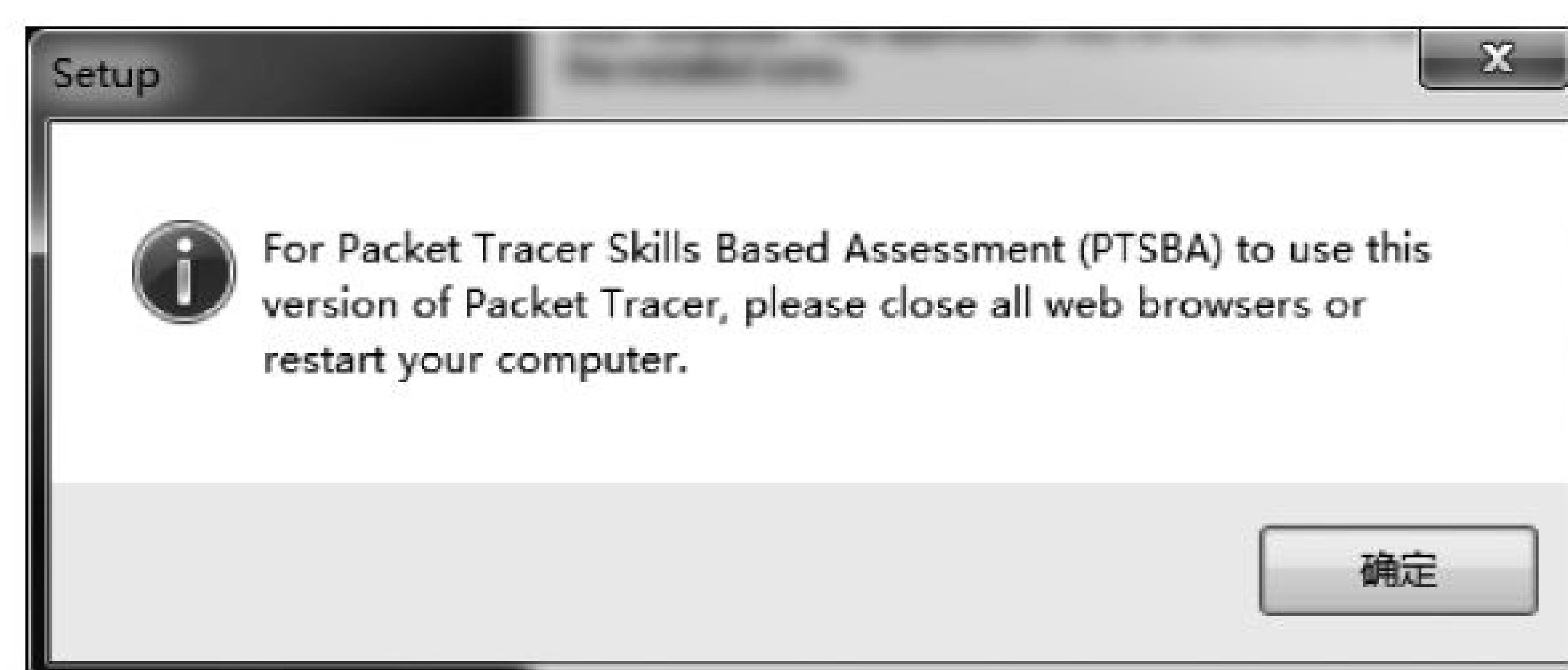


图 A-9　提示用户关闭所有浏览器或重新启动计算机

A.2 将工作界面修改为中文

第 1 次运行 Packet Tracer 7.0 时，计算机屏幕会出现用户注册页面，请按提示的要求填写个人相关的资料进行注册，注册完成后，会出现如图 A-10 所示的信息。

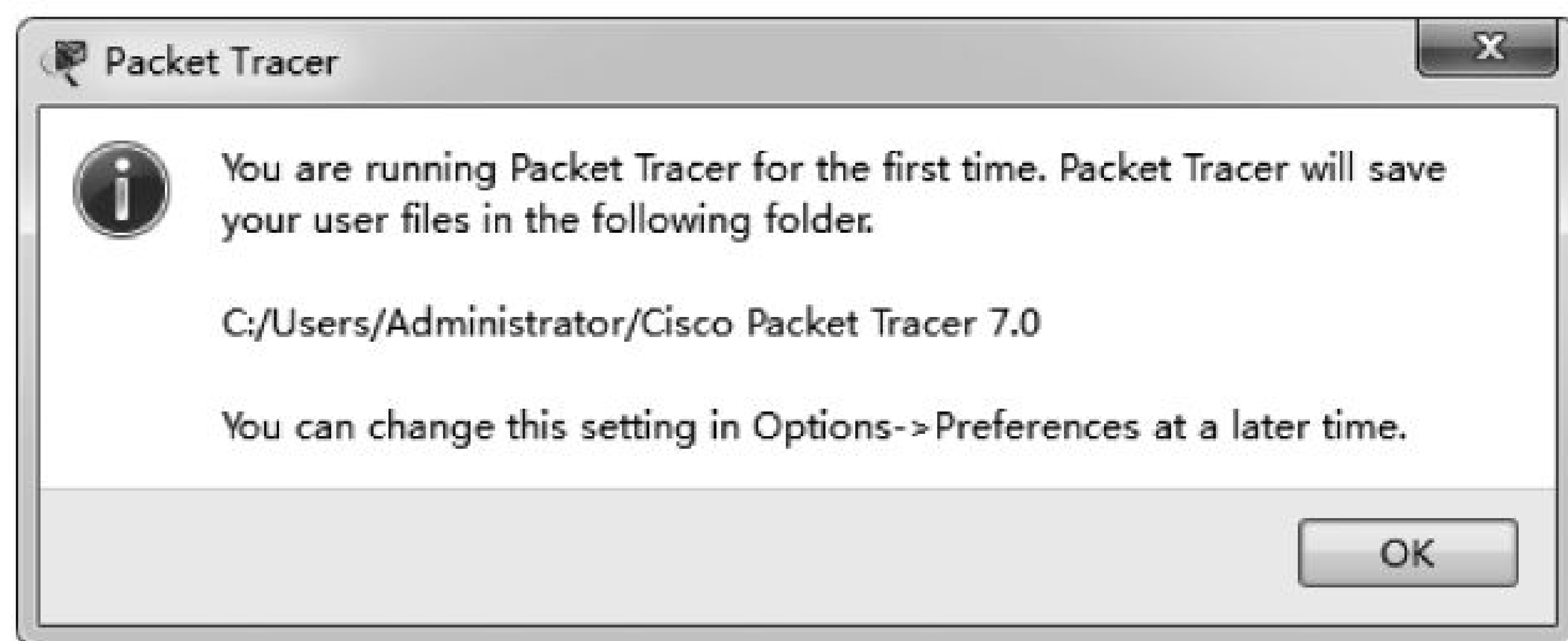


图 A-10 提示用户默认的文件保存路径

图 A-10 中显示的信息说明当前 Packet Tracer 7.0 用户默认的文件保存路径为 C:/Users/Administrator/Cisco Packet Tracer 7.0。如果用户需要修改文件默认的保存路径，可以进入菜单 Options，然后再进入子菜单项 Preferences 中进行修改。

启动 Packet Tracer 7.0 后，如果觉得软件的英文界面使用起来不够直观，可以通过指定使用的语言包的方法进行汉化，即把 Packet Tracer 7.0 的工作界面修改为中文，具体的设置步骤如下。

首先下载 Packet Tracer 7.0 专用的中文语言包，文件名为 chinese.ptl，并把这个文件复制到 C:\Program Files\Cisco Packet Tracer 7.0\languages 文件夹中，如图 A-11 所示。

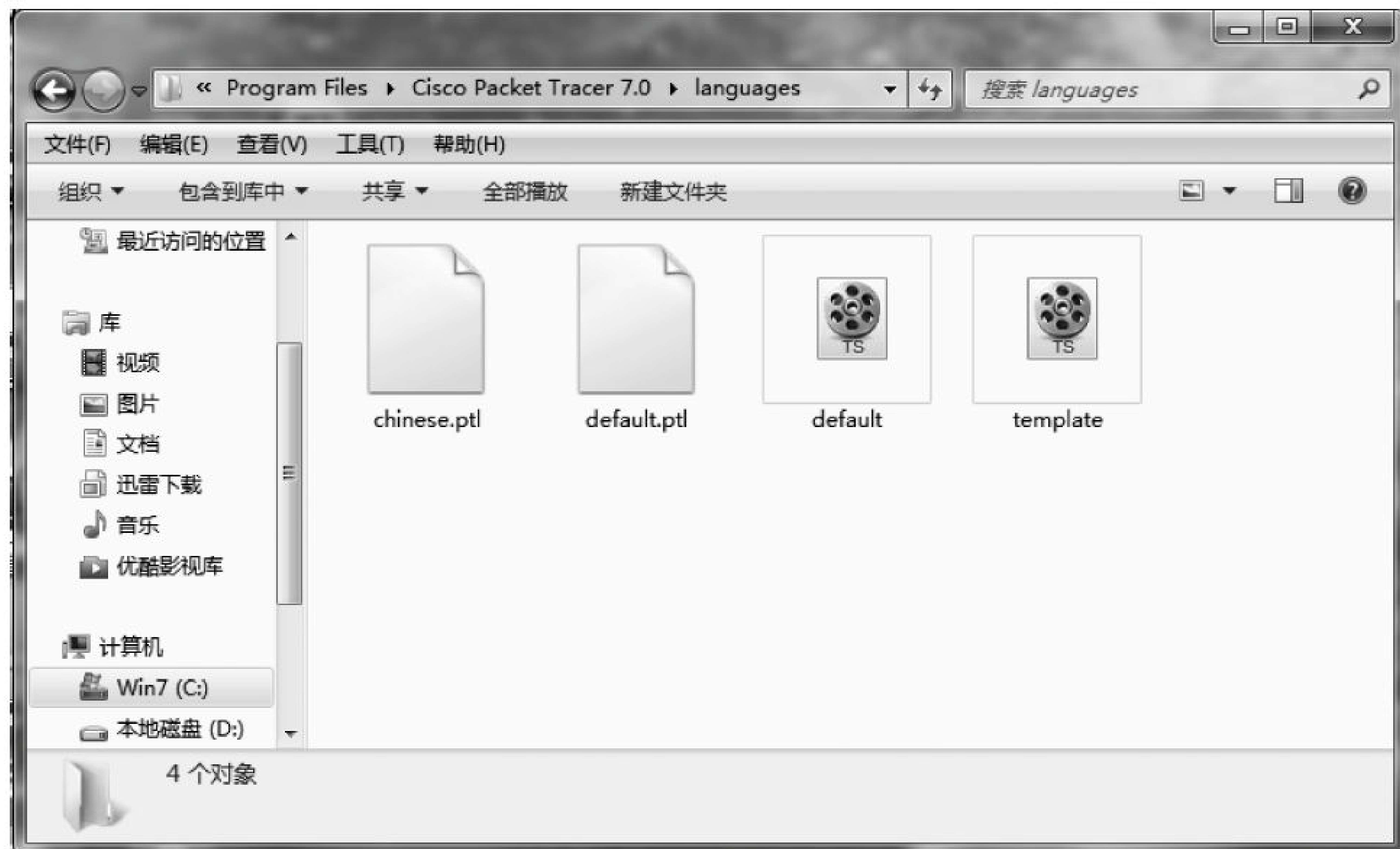


图 A-11 把中文语言包复制到 Packet Tracer 7.0 的指定文件夹

接着就可以启动 Packet Tracer 7.0 了。启动软件后，会显示如图 A-12 所示的英文工作界面。

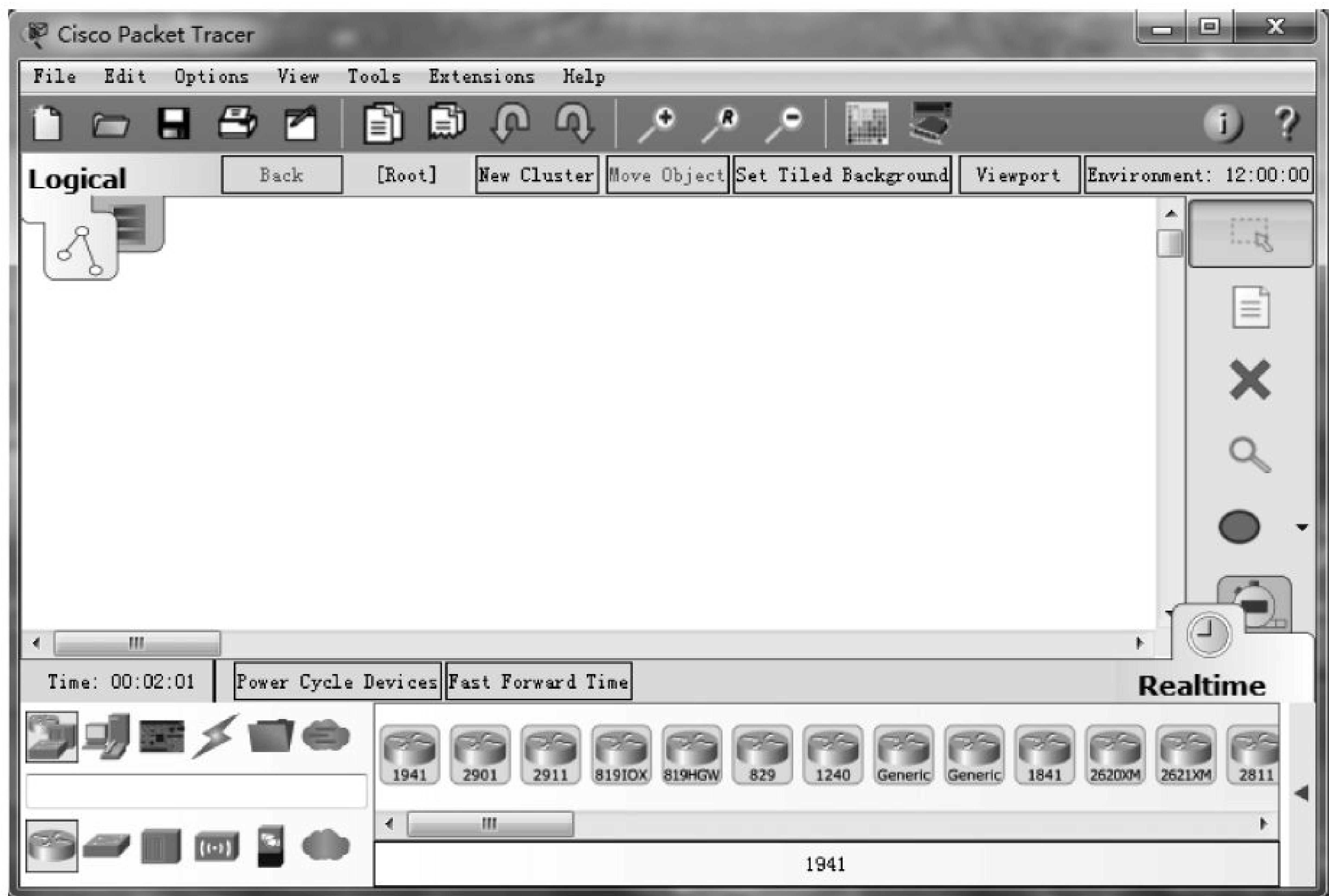


图 A-12　Packet Tracer 7.0 的工作界面

单击 Options 菜单项，打开 Options 菜单，如图 A-13 所示。

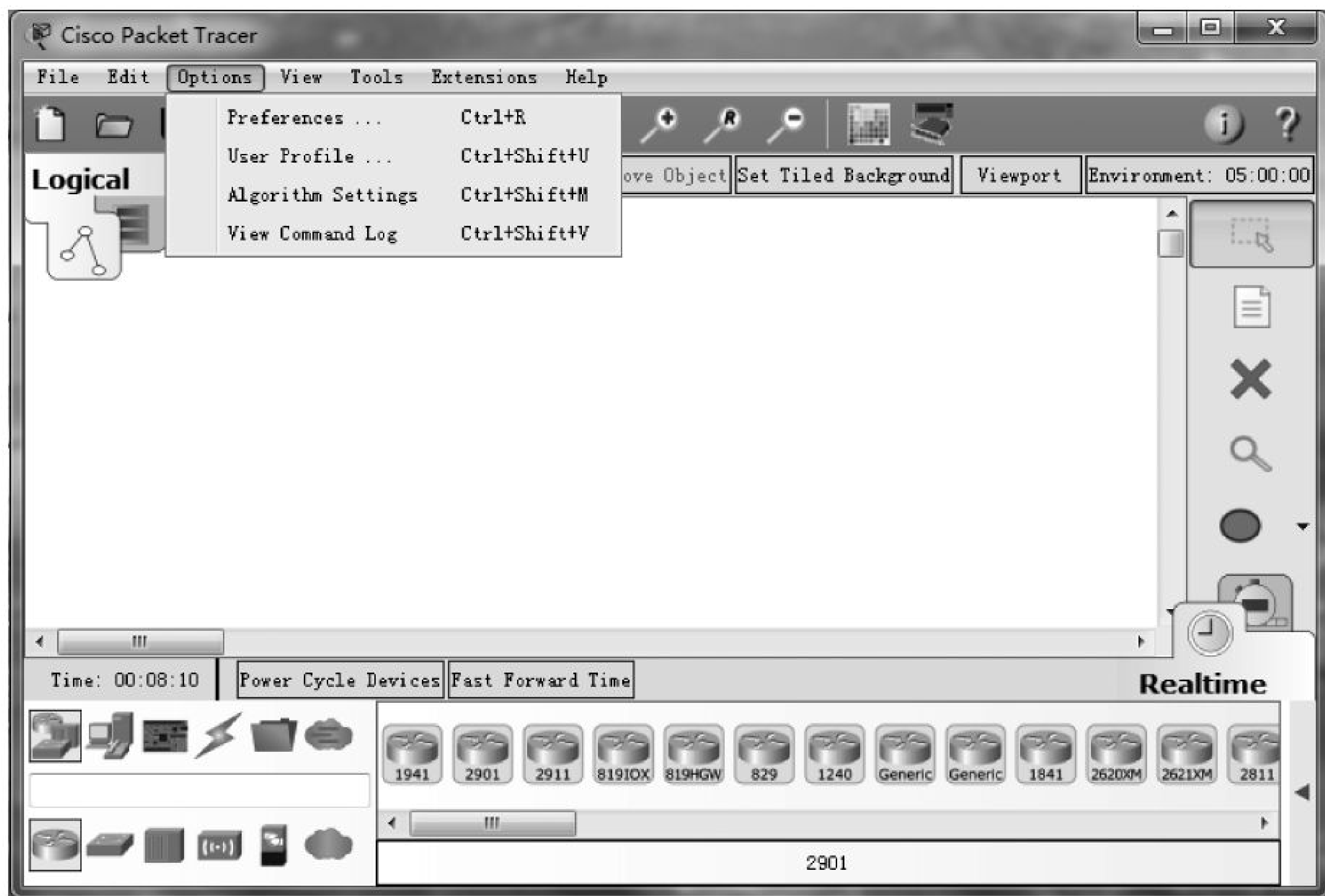


图 A-13　Packet Tracer 7.0 的 Options 菜单

单击 Options 菜单中的 Preferences，进入 Preferences 的设置页面，如图 A-14 所示。

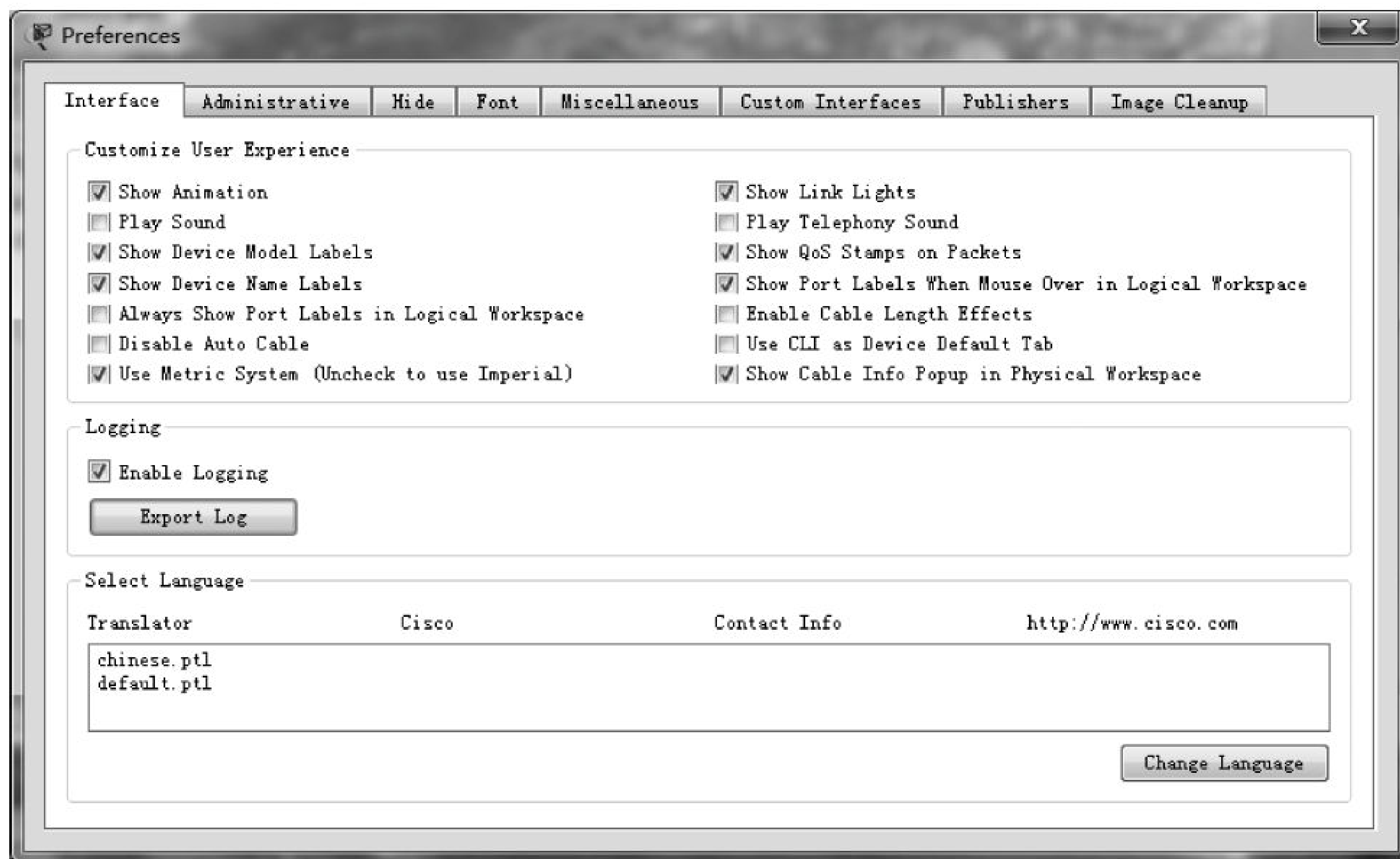


图 A-14 Preferences 的设置页面

单击页面左下方的 chinese.ptl，选定中文语言包，然后单击 Change Language 按钮，会出现如图 A-15 所示的提示信息。

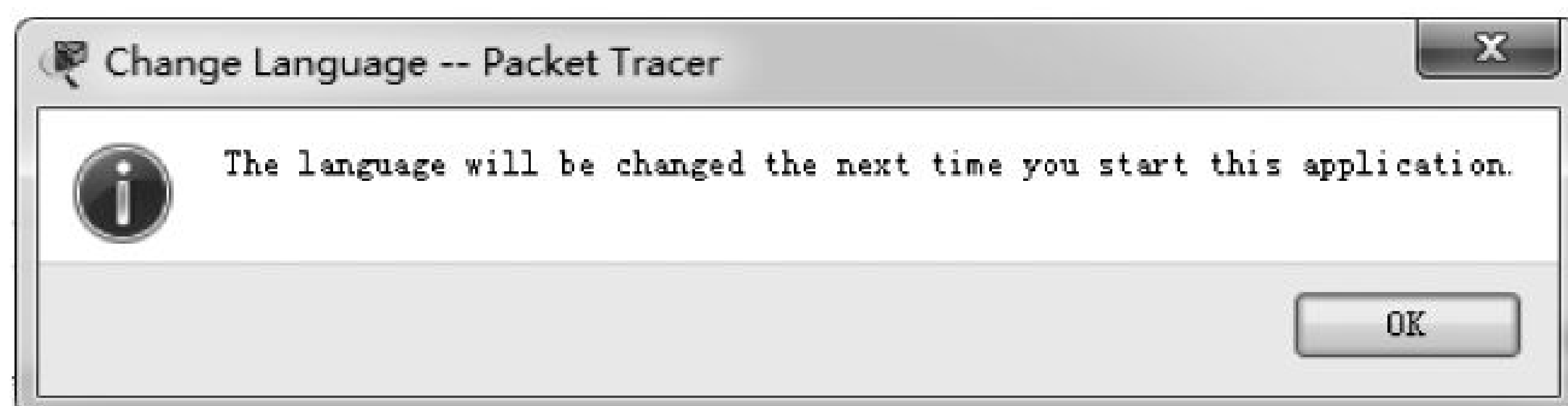


图 A-15 改变语言的提示信息

图 A-15 的提示信息是说明 Packet Tracer 7.0 所使用语言已经修改为中文，中文显示效果将在下次启动时生效。

注：因为 Packet Tracer 7.0 的中文语言包尚未完善，仍然未能实现全部汉化，所以 Packet Tracer 7.0 的工作界面中仍有许多地方显示为英文。

另外，由于汉字的字型比较复杂，字体太小的汉字会看不清楚，因此还需要继续设置汉字的字体。具体方法是单击 Options 菜单项，在打开的 Options 菜单中单击 Preferences，进入 Preferences 的设置页面。

接着单击 Font(字体)，出现如图 A-16 所示的字体设置页面。

在图 A-16 中，请按照页面的提示依次单击右侧的方向向下的黑色小三角形按钮，把"命令行""工作区""活动向导"和"按钮/标签"的字体大小设置为 12，最后单击页面下方的"应用"按钮完成字体的设置。

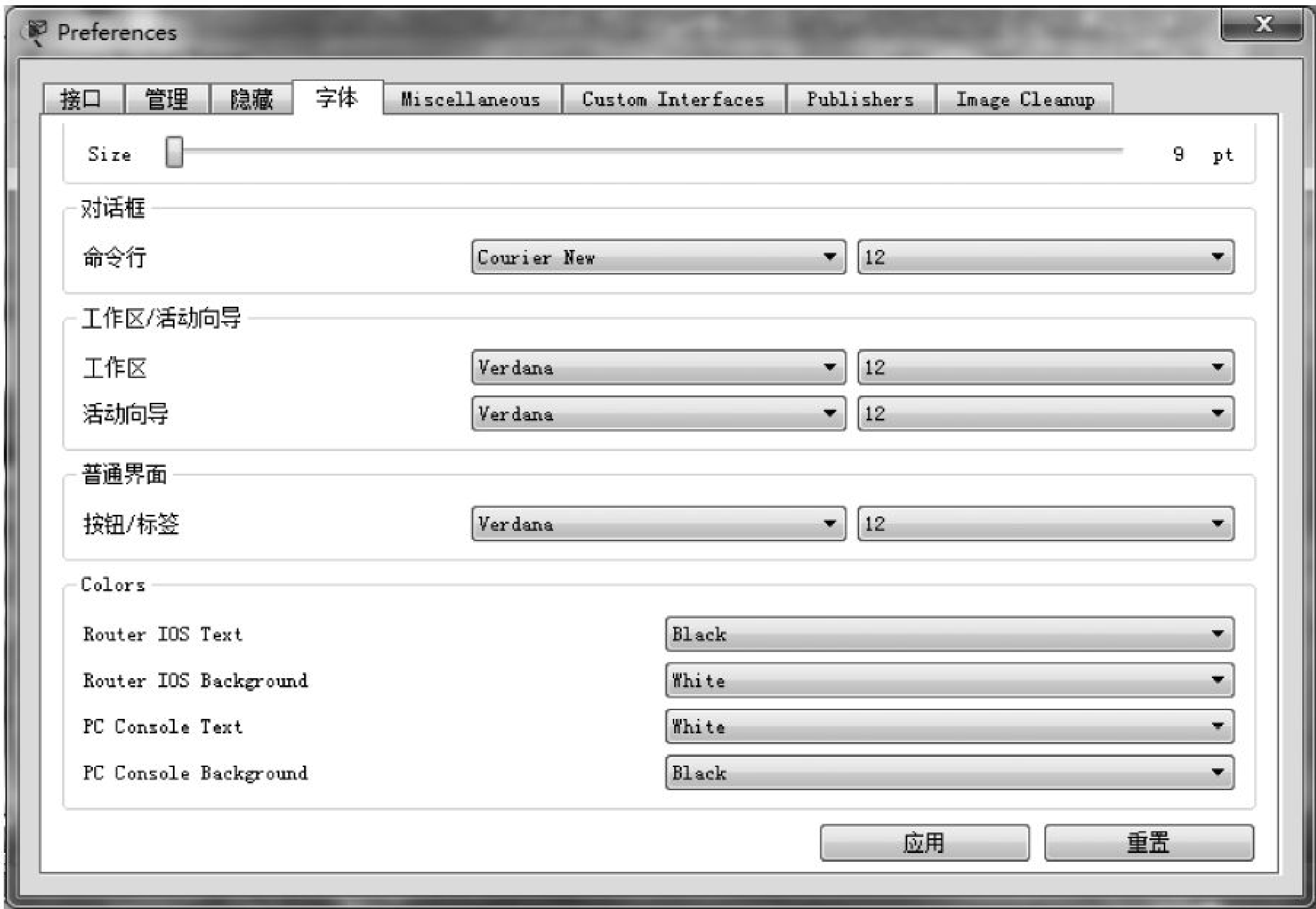


图 A-16 字体设置页面

A.3 Packet Tracer 7.0 的工作区域

如图 A-17 所示，Packet Tracer 7.0 的工作区域可以分为以下 8 个工作区域。

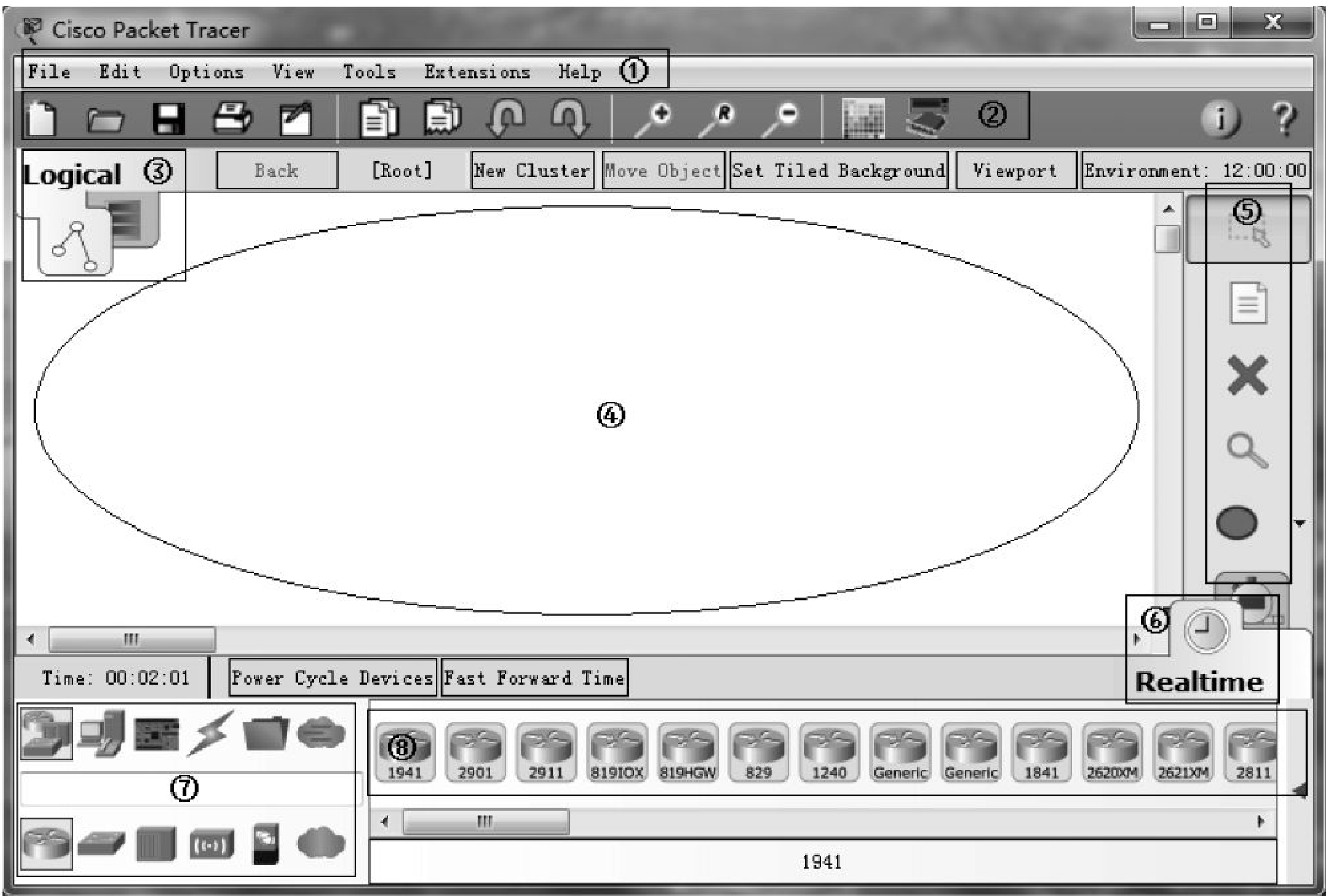


图 A-17 Packet Tracer 7.0 的工作区域

① 菜单栏：此栏中包括 File(文件)、Edit(编辑)、Options(选项)、View(视图)、Tools(工具)、Extensions(扩展)和 Help(帮助)菜单。

② 主工具栏：此栏中包括新建文件、打开文件、保存文件、打印等常用工具按钮。

③ 工作区转换栏：通过此栏中的按钮可以实现逻辑工作区与物理工作区的转换。

④ 工作区：中间的白色区域是工作区，可以在此区域中创建网络拓扑环境，监视网络设备的工作情况，查看各种信息和网络参数。

⑤ 常用工具栏：此栏中提供了选择工具、注释工具、删除工具、查看工具、作图(多边形、矩形、椭圆、直线)工具、调整图形大小工具等常用工具。

⑥ 实时模式/模拟模式转换栏：通过此栏中的按钮可实现实时模式与模拟模式之间的转换。

⑦ 设备类型栏：通过此栏中的按钮可以选择网络设备的类型，如连接线、路由器、交换机、集线器、无线设备、加密设备等。

⑧ 设备型号栏：通过此栏中的图标可选择具体型号的设备，如 2811 型路由器。

A.4 布置网络设备

在 Packet Tracer 7.0 的工作界面中布置网络设备的方法非常简单，直接用鼠标把设备型号栏中的网络设备图标拖到工作区中即可。

A.5 连接网络设备

把网络设备图标拖到工作区后，就可以选择适当的连接线将网络设备连接起来。在 Packet Tracer 7.0 中，各种不同的网络连接线对应的图标及其名称如图 A-18 所示。

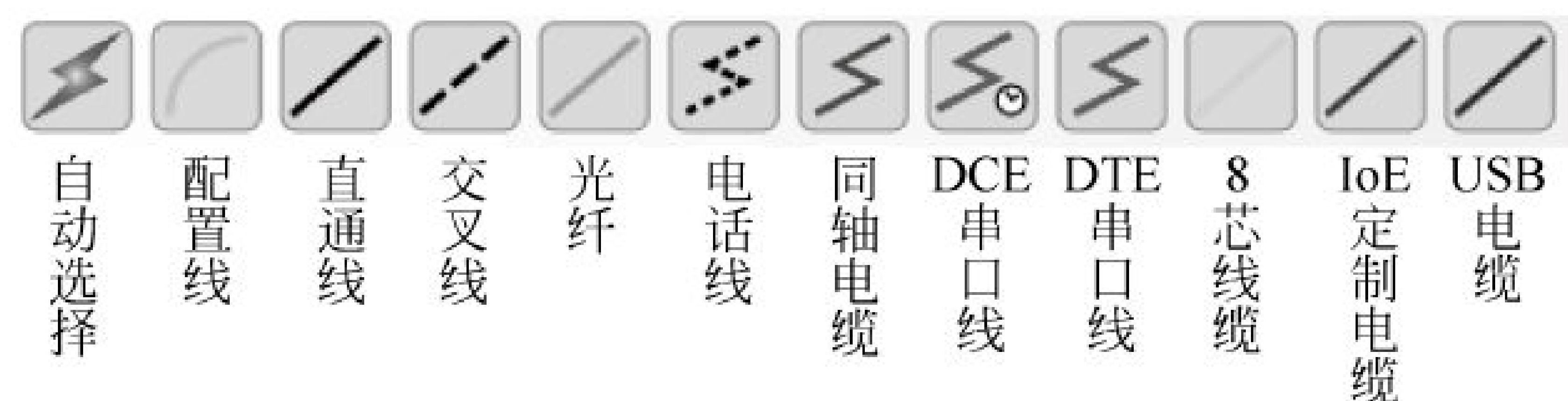


图 A-18 网络连接线对应的图标及其名称

配置网络硬件时，网络管理员应学习相关的硬件知识，掌握各种不同连接线的功能和特性，以便为网络设备选择合适的连接线。例如，超级终端与路由器之间要用配置线(浅蓝线)连接，交换机与路由器之间要用直通线(黑实线)连接，路由器与路由器之间要用交叉线(黑虚线)连接。

准确地说，同类型的端口相连要用交叉线，而不同类型的端口相连要用直通线。例如，一台交换机的 UPLINK 端口要与另一台交换机的普通端口相连(即级联)时，虽然两者是同种设备，但是却要用直通线连接。

在 Packet Tracer 7.0 中模拟实际的网络环境连接网络设备非常简单，具体方法如下：首先用鼠标选择正确的连接线，然后将鼠标移到第一台设备的图标处，页面中就会出现若干个可供连接的接口；此时请按网络布线的实际需求用鼠标选择适当的接口，然后继续将鼠

标移到另一台设备的图标处，则页面中又会出现若干个可供连接的接口；同样用鼠标选择适当的接口即可。

图 A-19 是一个简单的网络设备连接的实例。

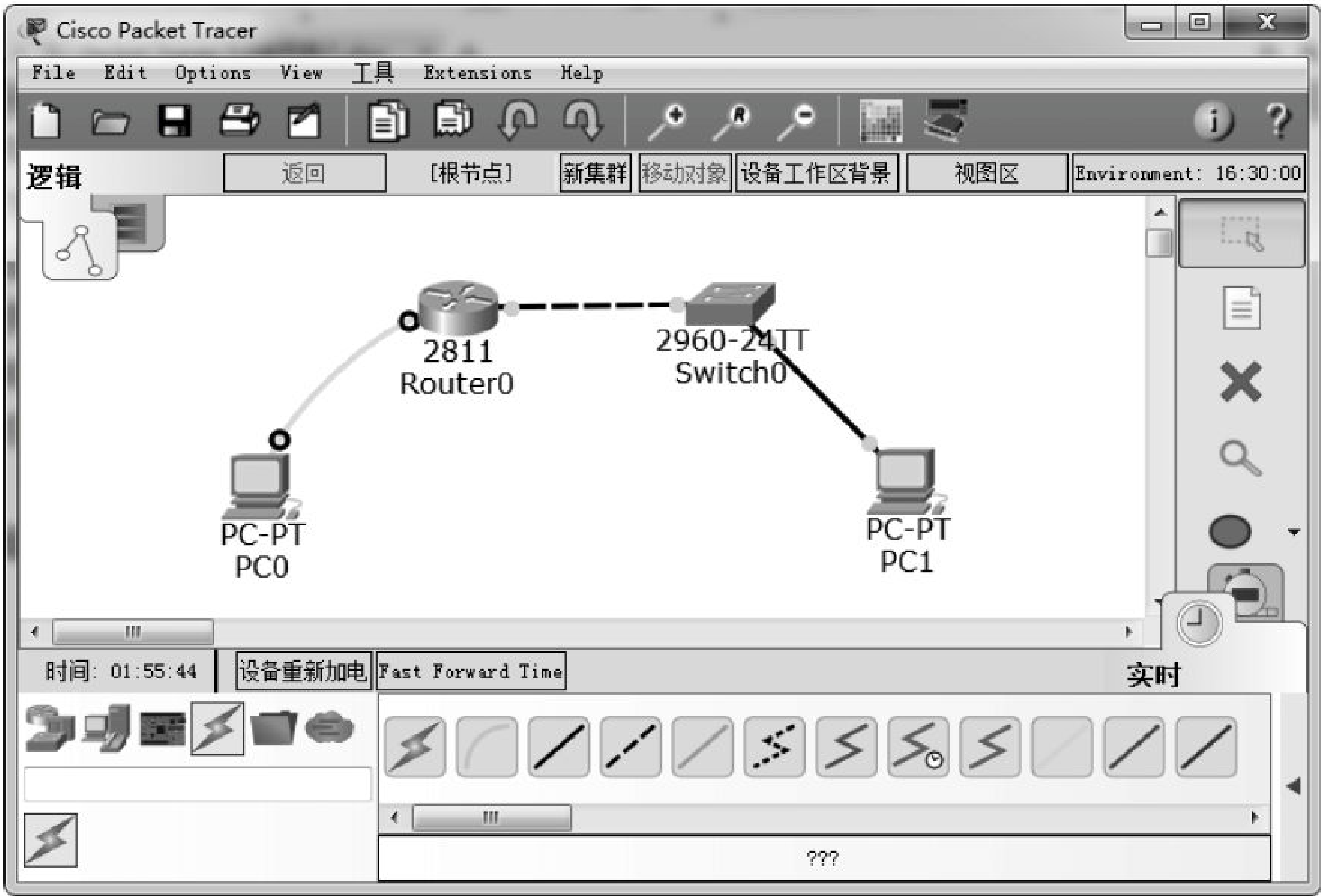


图 A-19　简单的网络设备连接的实例

在图 A-19 中，共有一台路由器、一台交换机和两台计算机。其中，计算机 PC0 作为超级终端，用于配置路由器参数，其 RS232 串行接口通过配置线（浅蓝线）与路由器的 Console 接口连接；路由器的快速以太网接口 0/0 通过交叉线（黑虚线）与交换机的快速以太网接口 0/1 连接；而交换机的快速以太网接口 0/2 通过直通线（黑实线）与计算机 PC1 连接。

设备连接以后，每条线缆两端都会出现不同颜色的圆点，这些圆点的含义如表 A-1 所示。线缆两端圆点的不同颜色揭示了网络当前连接的状态，这有助于管理员排除网络连通性的故障。

表 A-1　线缆两端圆点颜色的含义

线缆两端圆点的颜色	含　　义
亮绿色	物理连接就绪
闪烁绿色	连接激活
红色	物理连接不通，没有信号
黄色	交换机端口处于“阻塞”状态

A.6　配置网络设备

网络设备连接好后，就需要逐个配置网络设备参数了。例如，配置接口的 IP 地址和子网掩码等。具体方法是单击工作区中的网络设备图标，在弹出的配置页面中设置。

1）配置路由器

这里仍以图 A-19 中所示的网络设备为例，单击工作区中的路由器图标，会出现如图 A-20 所示的页面，包含 Physical、Config、CLI、Attributes 选项卡。



图 A-20　路由器配置页面

在图 A-20 中，Physical（物理）选项卡用于添加端口模块。页面左侧列出了各种模块的名称，下方给出了每种模块的简要说明。如果需要添加某个模块，请首先关闭路由器的电源，然后直接把模块拖到右边的插槽（即黑色区域）中，最后重新开启路由器的电源，即可完成添加模块的操作。

在图 A-20 中，单击 Config（配置）按钮可以进入 Config 选项卡，如图 A-21 所示。Config 选项卡提供了便捷配置路由器的图形化界面，在这里可以设置接口的 IP 地址、子网掩码和激活状态等参数。当进行某项配置时，页面下方会同步显示相应的命令。注意：这是 Packet Tracer 的便捷配置方式，可便于初学者进行操作，使初学者将注意力集中在配置参数上，但是实际设备是没有这种图形化界面的。在图 A-21 中，当把快速以太网接口 FastEthernet0/0 的 IP 地址设置为 A 类地址 10.10.10.1 时，则子网掩码会自动填写为 255.0.0.0。

CLI（命令行）选项卡的界面与真实路由器的配置界面相似，如图 A-22 所示。

2）配置计算机

在图 A-19 中，单击工作区中的 PC1 图标，会出现如图 A-23 所示的计算机配置页面，包含 Physical、Config、Desktop、Attributes 和 Software/Services 选项卡。

单击 Config，进入如图 A-24 所示 Config（配置）的 Global Settings（全局设置）页面，即可配置 Gateway（网关）、DNS Server（域名解析服务器）等地址参数。

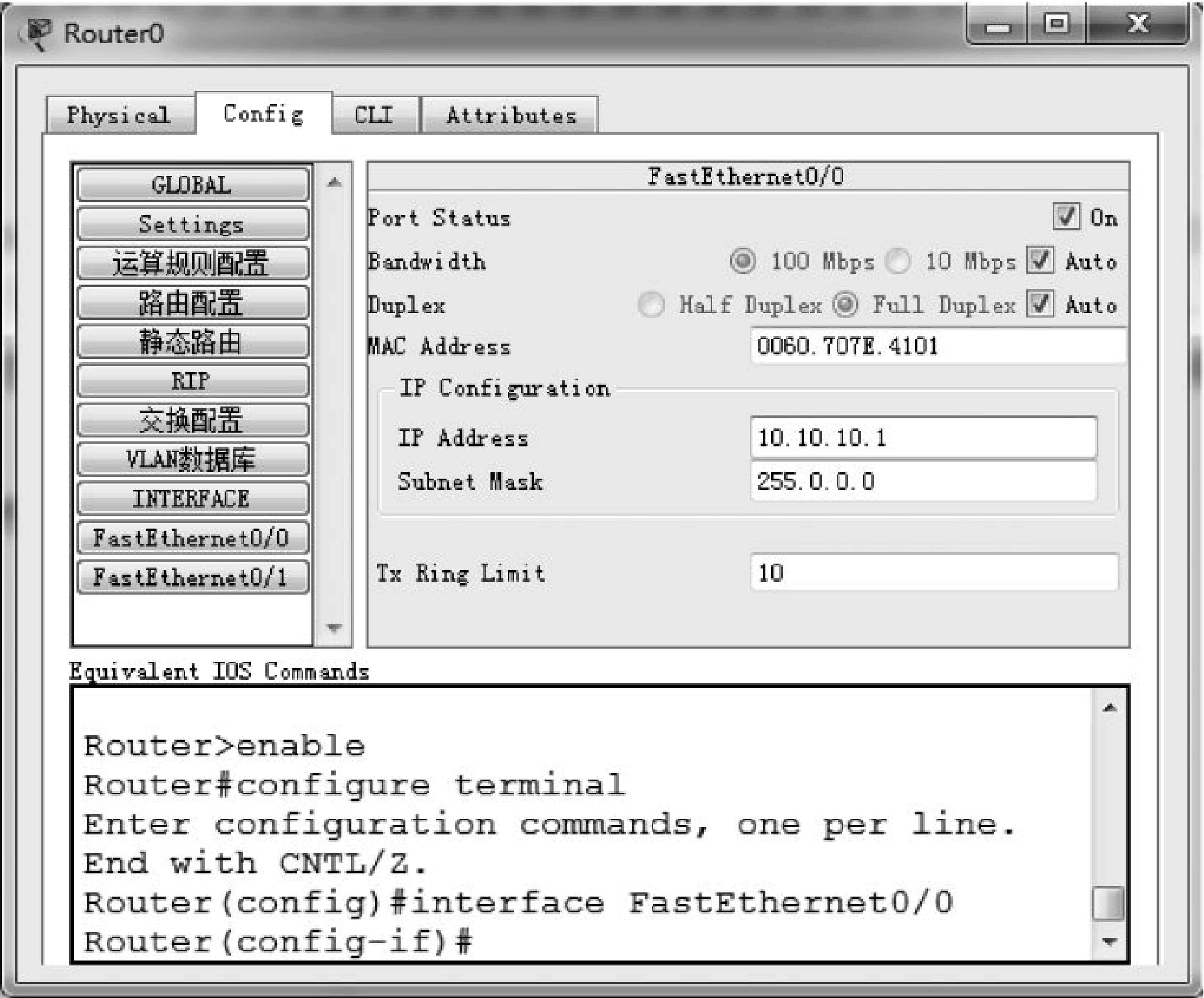


图 A-21　Config(配置)选项卡

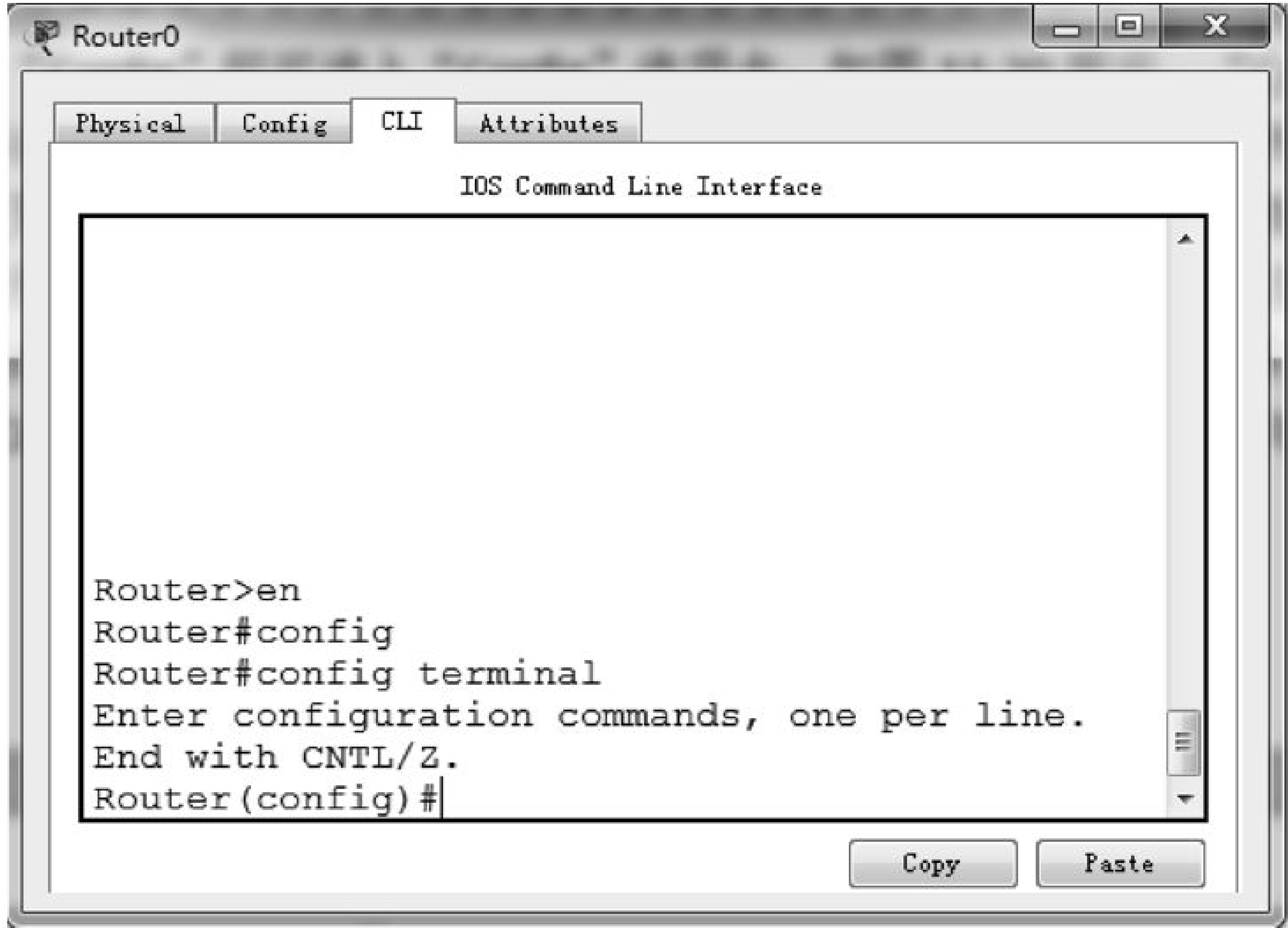


图 A-22　CLI(命令行)选项卡

单击 FastEthernet0 按钮进入如图 A-25 所示的 FastEthernet0 接口设置页面,即可配置计算机的 IP 地址、子网掩码等参数。

计算机并不像路由器那样有 CLI(命令行),如果点击 Desktop(桌面),可以进入如图 A-26 所示的桌面选项页面。

在图 A-26 所示的页面中,单击 Command Prompt 按钮即可进入计算机的 DOS 命令行工作模式,如图 A-27 所示。



图 A-23　计算机 Physical(物理)选项卡页面

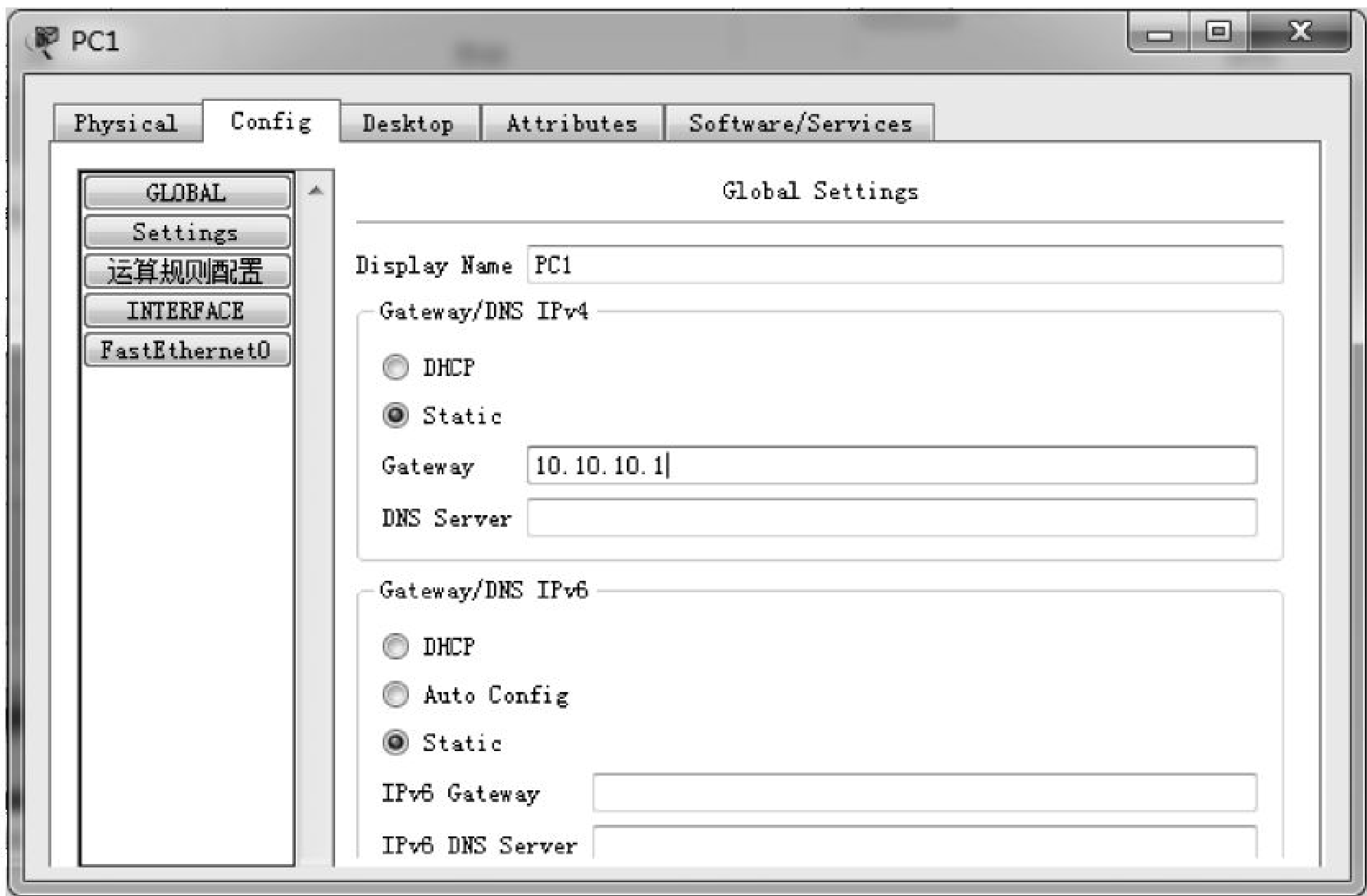


图 A-24　计算机 Config(配置)选项卡页面

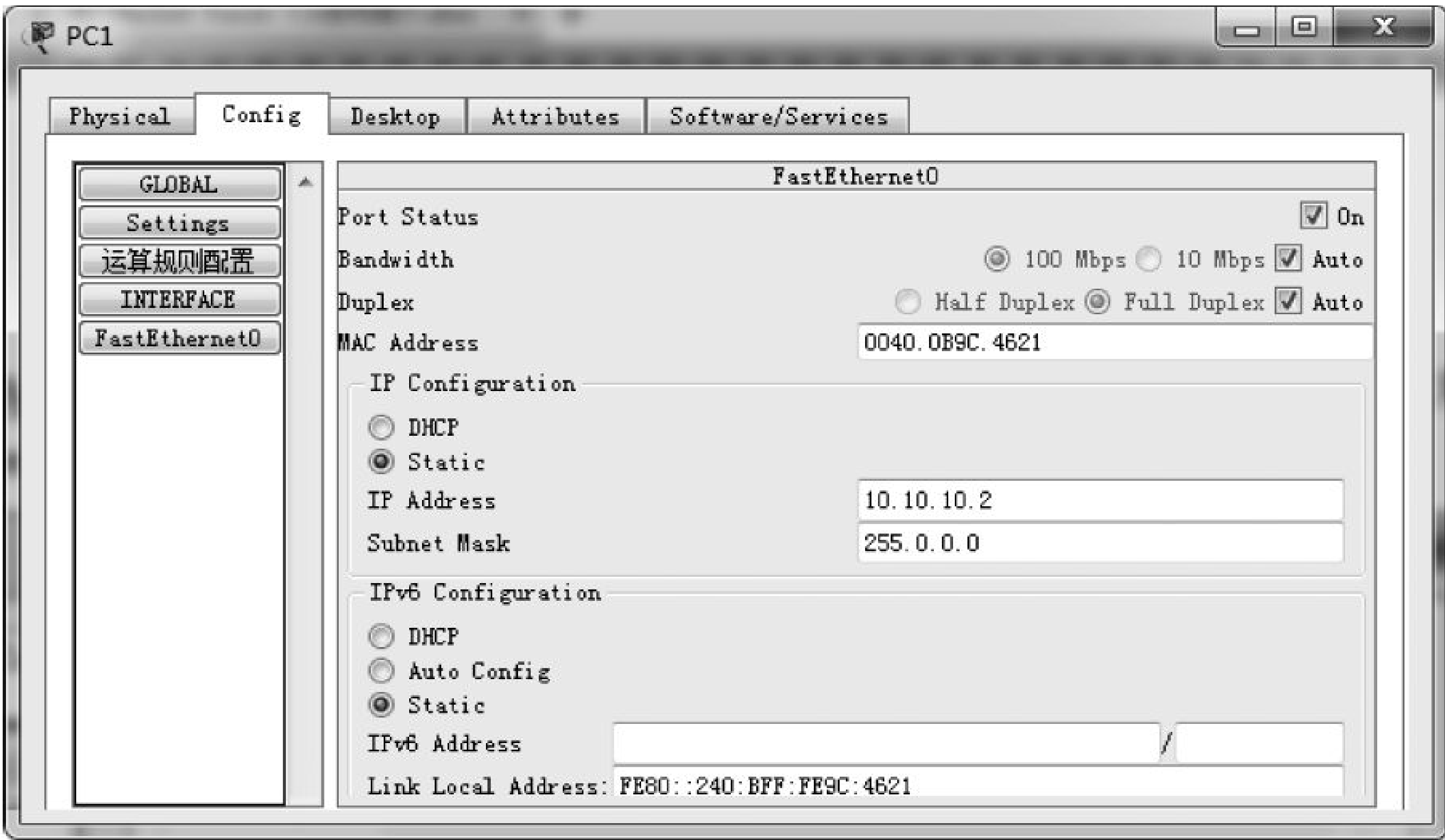


图 A-25 FastEthernet0 接口设置页面



图 A-26 桌面选项页面

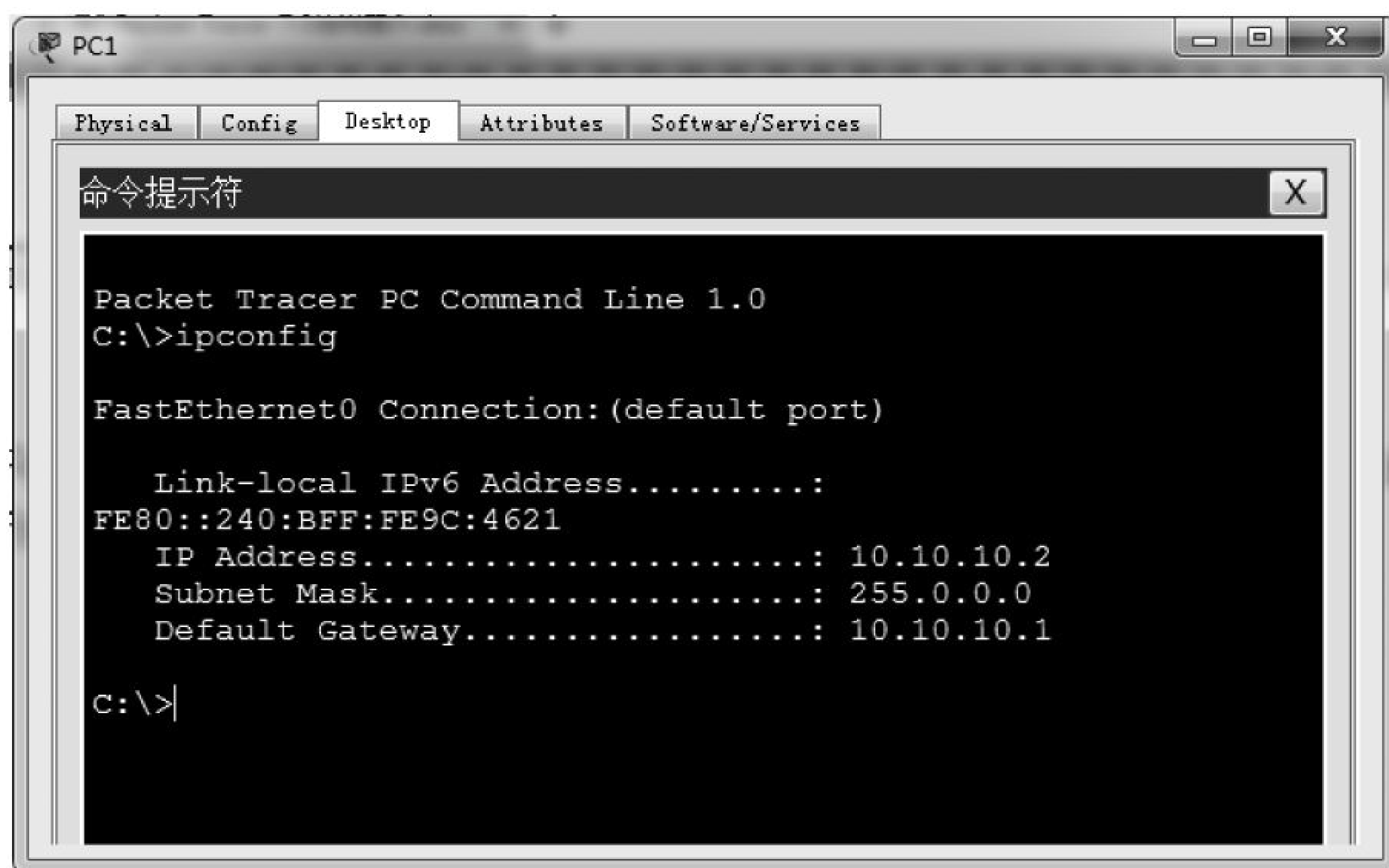


图 A-27 DOS 命令行工作模式

A.7 模拟模式

单击 Packer Tracer 工作界面的右下角 Simulation 按钮即可进入如图 A-28 所示的模拟模式。此时，单击“自动捕获/播放”按钮，可演示数据包的传输过程，这有助于初学者对网络设备的工作原理有更深入的了解。

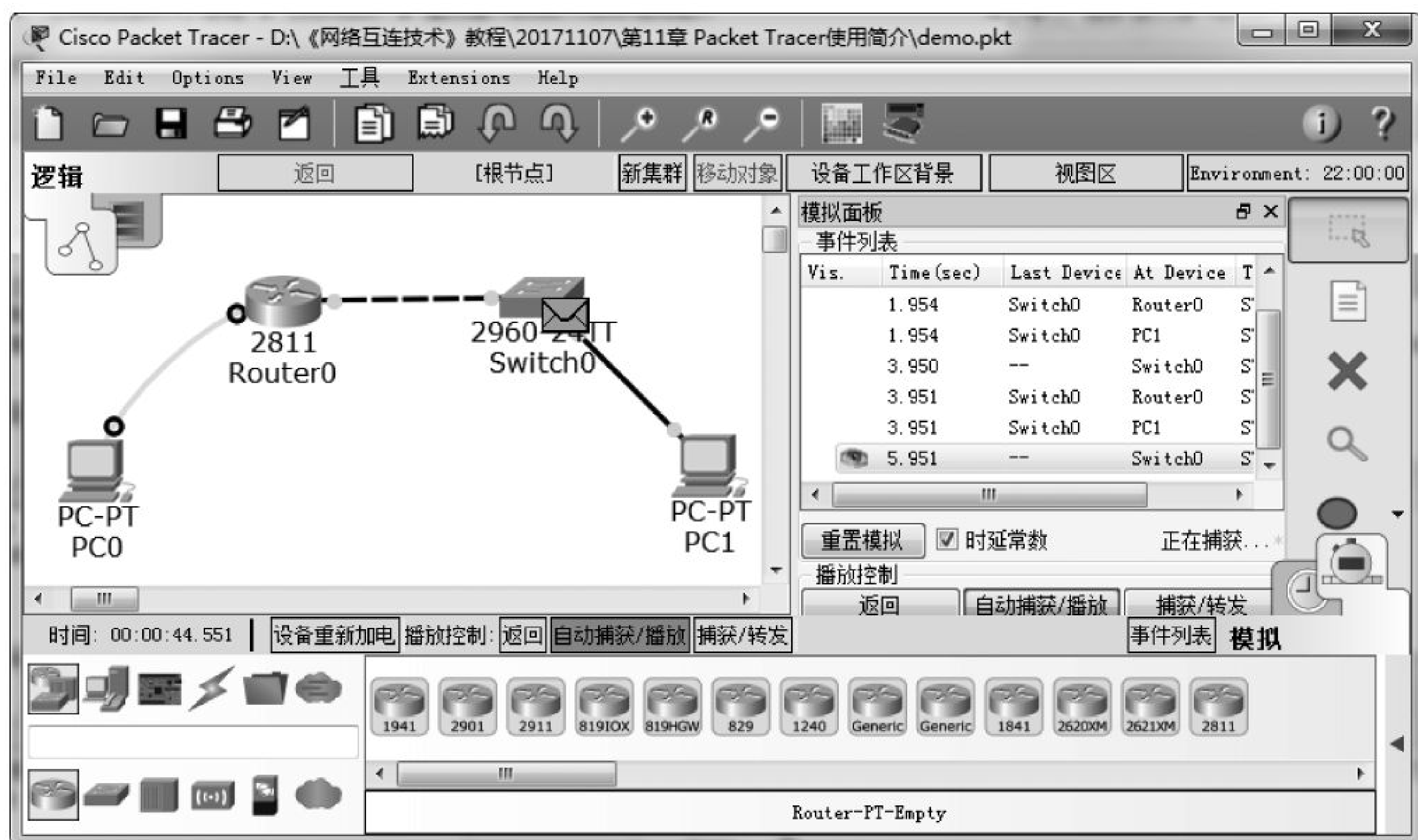


图 A-28 模拟模式的工作页面

A.8 Packet Tracer 的帮助文件

这里仅简要地介绍了 Packet Tracer 的基本操作。如果读者希望进一步学习 Packet Tracer，请如图 A-29 所示，单击 Packer Tracer 工作界面中的 Help 菜单中的 Contents 选项，打开 Packet Tracer 的帮助文件详细阅读。

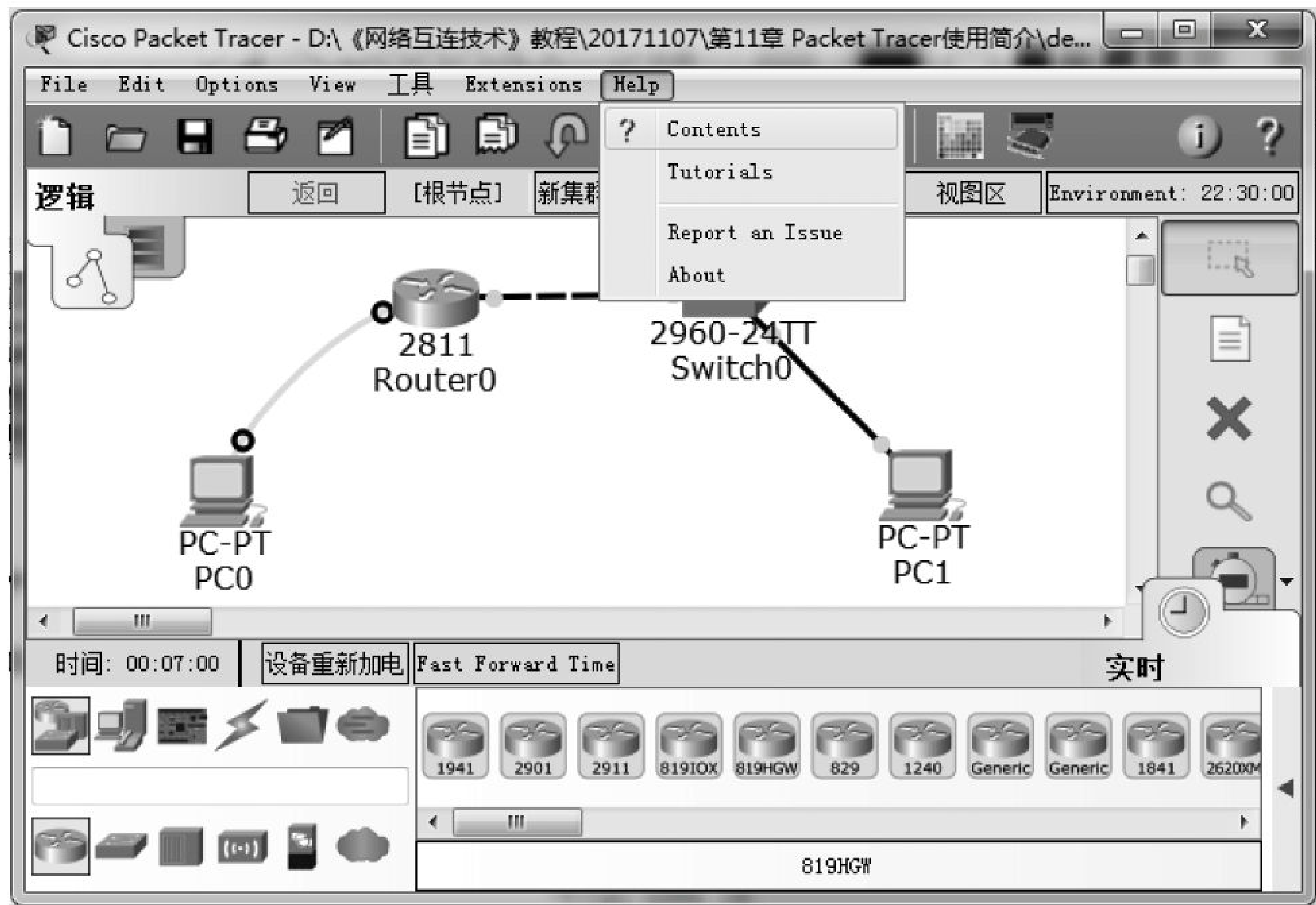


图 A-29 打开帮助文件

附录 B

APPENDIX B

模拟试题

B.1 模拟试题一

一、单项选择题(每小题 2 分,本题共 40 分)

1. 在 TCP/IP 协议栈模型中只有 4 层,即应用层、传输层、(　　)和主机到网络层。

   A. 物理层　　B. 网络互联层

   C. 数据链路层　　D. 主机到链路层

2. OSPF 是(　　)的协议。

   A. 应用层　　B. 传输层　　C. 网络互联层　　D. 以上都不是

3. (　　)不属于路由器硬件。

   A. AUX　　B. FLASH　　C. NVRAM　　D. 硬盘

4. RIP 使用的端口号是(　　)。

   A. 500　　B. 510　　C. 520　　D. 530

5. 路由器与以太网交换机之间通过(　　)连接。

   A. 直通线　　B. 交叉线　　C. 控制线　　D. USB 线

6. CLI 提示符 R1(config-if)表示(　　)。

   A. 用户模式　　B. 特权模式

   C. 全局配置模式　　D. 接口配置模式

7. (　　)是一种外部网关协议。

   A. RIP　　B. IGRP　　C. OSPF　　D. BGP

8. 以下不属于路由器技术的是(　　)。

   A. RIP　　B. VLAN　　C. ACL　　D. OSPF

9. 192.168.0.1 属于(　　)IP 地址。

   A. A 类　　B. B 类　　C. C 类　　D. D 类

10. conf t 命令的作用是(　　)。

    A. 进入普通用户模式　　B. 进入特权用户模式

    C. 进入接口配置模式　　D. 进入全局配置模式

11. shutdown 命令的作用是(　　)。

    A. 启动接口　　B. 关闭接口　　C. 启动路由器　　D. 关闭路由器

12. 设置路由器从普通用户模式进入特权用户模式明文密码的命令是(　　)。

A. enable password password　　B. enable secret password

C. set password password　　D. set secret password

13. 进入特权用户模式的明文密码可以用(　　)命令查看。

A. show password　B. show secret　C. show flash　D. show run

14. 进入路由器辅助接口配置模式的命令是(　　)。

A. line console 0　B. line aux 0　C. line tty 0 4　D. line vty 0 4

15. IPv6 地址由 128 位二进制数组成,为了方便表示,这 128 位的二进制数用(　　)将其分割成 8 个位域,每个位域包含 4 个 4 位的十六进制数。

A. 逗号　B. 分号　C. 实心句号　D. 冒号

16. 为了实现 IPv4 向 IPv6 升级时的平稳过渡,主要采用(　　)种不同的机制。

A. 3　B. 4　C. 5　D. 6

17. TFTP 服务器的作用是(　　)。

A. 备份和恢复路由器配置文件　　B. 备份和恢复交换机配置文件

C. 备份和恢复路由器或交换机配置文件　　D. 以上都不是

18. 由路由器管理人员手工配置的静态路由与路由器通过动态选择协议学习到的路由信息相比,静态路由更(　　)。

A. 可靠　　B. 不可靠

C. 可靠性一样　　D. 可靠性无法比较

19. 无类路由协议包括 RIPv2 和(　　)。

A. OSPF　B. RIPv1　C. IGRP　D. ICMP

20. 不属于 EIGRP 工作原理的是(　　)。

A. 可靠传输协议　　B. 扩散更新算法

C. 邻居的发现/恢复　　D. 更新计时器

二、判断题(正确的打√,错误的打×,每小题 1 分,本题共 10 分)

1. RIPv2 的跳跃计数的最大值与 RIPv1 的跳跃计数的最大值一样,不可以支持更大的网络规模。(　　)

2. RIP 有 4 个版本,即 RIP、RIPv2、RIPv3、RIPng。(　　)

3. copy running-config ftp 命令的作用是备份路由表到 FTP 服务器。(　　)

4. network 命令仅用于配置静态路由。(　　)

5. 解决路由环路问题的常见方法有计数到无穷、水平分割、触发更新、路由毒杀和反转毒杀、抑制定时器等。(　　)

6. Cisco 定义的 OSPF 最多可以支持 6 条等值路径,由这 6 等值路径平均分担网络流量。(　　)

7. EIGRP 数据包共有 4 种类型。(　　)

8. 配置 RIPng 协议时不再使用 network 命令。(　　)

9. show ip route 命令用于查看 IPv6 路由表。(　　)

10. Windows 7 系统已经自带了配置路由器的超级终端程序。(　　)

三、填空题(每空 1 分,本题共 10 分)

1. 路由器的 RIPv1 协议的配置方法很简单,相关的 RIPv1 基本配置命令是__________、__________,RIP 基本诊断命令是__________、__________。

2. 执行 ping 命令后显示的结果是 1 个实心圆点和 4 个感叹号,其含义是指__________和__________。

3. 配置 RIP 路由器动态路由负载分担的方法是____________________。

4. ip route 命令的作用是____________________。

5. interface fastethernet 命令的作用是____________________。

6. Cisco 从 iOS ________________版本开始支持命名 ACL。

四、名词解析(每个名词 5 分,本题共 10 分)

1. OSPF 协议

2. ISATAP 隧道

五、简答题(每小题 3 分,本题共 12 分)

1. 假设路由器原来的名字是 CISCO,要求将路由器的名字修改为 Router,请写出相关的命令(注意:要写出完整的提示符)。

2. 设置路由器从普通模式进入特权模式的密文密码为 netuser2018,请写出完整的提示符和相关命令。

3. 设置路由器的串行接口 Serial 0/0 的 IP 地址为 10.10.10.10,时钟频率为 128 000Hz,并激活接口;设置串行接口 Serial 0/1 的 IP 地址为 20.20.20.20,时钟频率为 128 000Hz,并激活接口。请写出相关命令。

4. 为路由器配置 RIPv2 协议。请写出相关命令。

六、综合题（本题共 18 分）

① 如图 B-1 所示，超级终端与路由器 A 之间用什么连接线？超级终端连接线应分别接到超级终端与路由器的什么接口？两路由器之间要用什么连接线？路由器与交换机之间又要用什么连接线？（4 分）

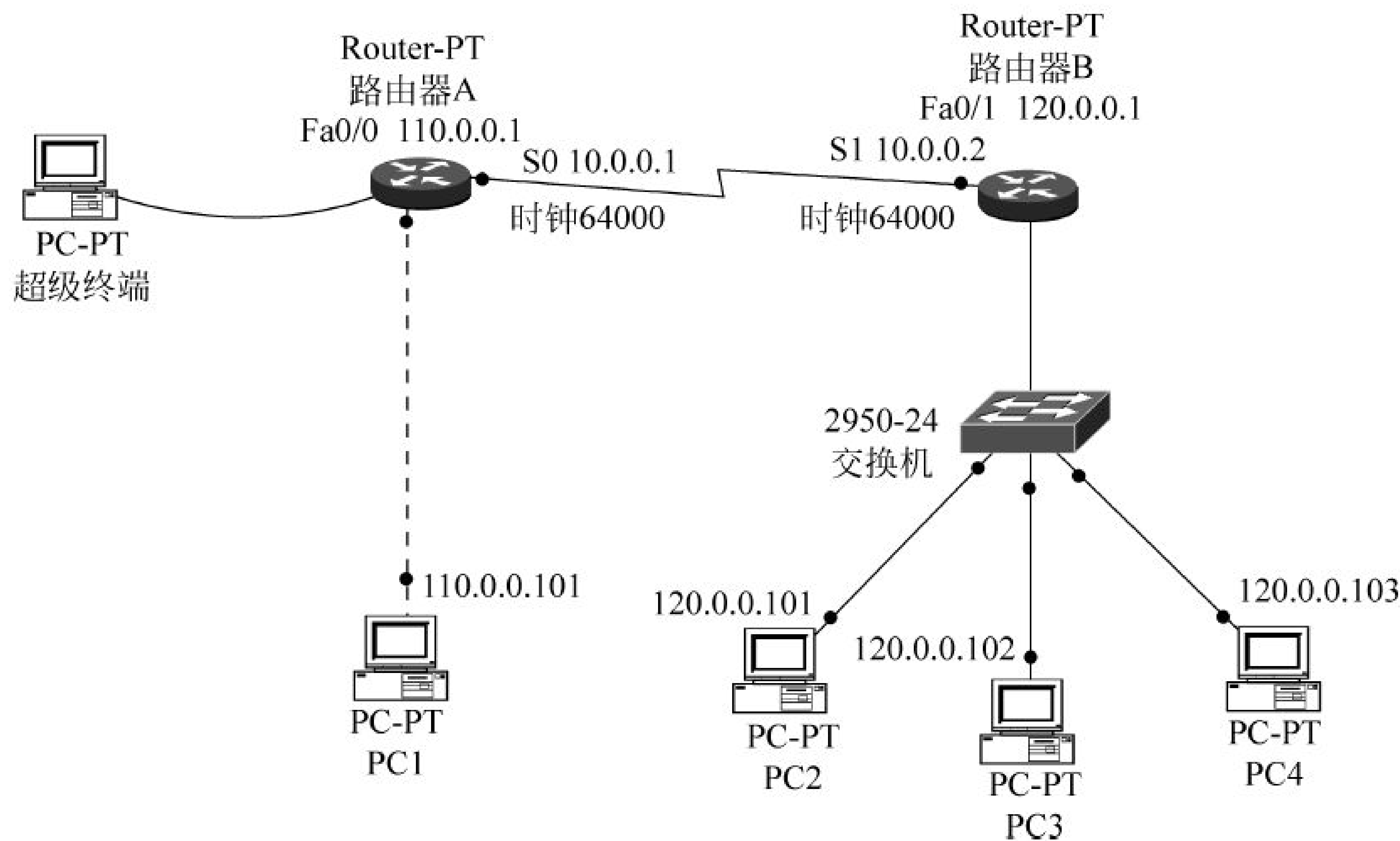


图 B-1

② 请按图 B-1 所示的网络环境配置路由器 A 串行接口 S0 和快速以太网接口的参数，并给出相关的配置命令。（4 分）

③ 请按图 B-1 配置计算机 PC1 的网络接口的参数，给出相关的配置命令或方法，并给出测试网络接口参数的方法。（4 分）

④ 如图 B-1 所示，分别给出配置路由器 A、B 的工作模式为 OSPFv3 的命令，并给出测试网络的连通性的相关命令。（6 分）

B.2 模拟试题二

一、单项选择题(每小题 2 分,本题共 40 分)

1. TCP/IP 协议栈模型中只有 4 层,最高层为(　　)。

A. 应用层　　B. 网络互连层
C. 数据链路层　　D. 主机到链路层

2. RIPng 是(　　)的协议。

A. 应用层　　B. 传输层　　C. 网络互连层　　D. 数据链路层

3. 邻居发现协议使用(　　)种类型的 ICMP 数据包。

A. 2　　B. 3　　C. 4　　D. 5

4. 在 IPv6 地址中,连续多个 0 可能使用(　　)表示。

A. 实心圆点　　B. 分号　　C. 冒号　　D. 双冒号

5. 命令 access-list 的作用是配置(　　)。

A. 隧道　　B. 接口　　C. 访问控制列表　　D. 静态路由

6. 在命令 showip route 返回的信息中,如果某一行以字母(　　)开头,则代表该行的路由信息是由 EIGRP 生成的。

A. C　　B. D　　C. E　　D. O

7. (　　)是一种不可靠的网络协议。

A. ICMP　　B. TCP　　C. UDP　　D. CSMA/CA

8. 以下表示访问控制列表的是(　　)。

A. RIP　　B. OSPF　　C. ACL　　D. VLAN

9. EIGRP 使用的多播地址是(　　)。

A. 224.0.0.10　　B. 224.0.0.20
C. 224.0.0.30　　D. 224.0.0.40

10. 命令 interfacefastethernet 的作用是(　　)。

A. 进入普通用户模式　　B. 进入特权用户模式
C. 进入接口配置模式　　D. 进入全局配置模式

11. no shutdown 命令的作用是(　　)。

A. 启动接口　　B. 关闭接口
C. 启动路由器　　D. 关闭路由器

12. 设置路由器从特权用户模式返回普通用户模式的命令是(　　)。

A. end　　B. exit
C. Disable　　D. 以上选项均可

13. EIGRP 综合了链路状态和距离矢量型路由选择协议这两种技术,采用(　　)算法来实现快速收敛。

A. 扩散更新　　B. 散列　　C. 聚合　　D. 距离矢量

14. OSPF 采用链路状态路由选择算法,用于在(　　)自治系统(Autonomous System)中进行决策路由。

A. 单一　　B. 两个
C. 多个　　D. 个数不限的

15. IPv6 地址由(　　)位二进制数组成。
A. 32　　B. 48　　C. 64　　D. 128

16. (　　)协议不能在算法上保证没有路由环路问题。
A. OSPF　　B. RIP　　C. EIGRP　　D. BGP

17. 在 ping 命令返回的结果中,代表网络连接正常的符号是(　　)。
A. 实心圆点　　B. 感叹号
C. 冒号　　D. 以上都不是

18. RIP 解决路由环路问题的方法主要为 6 种,即定义最大值、(　　)、路由中毒、反向路由中毒、控制更新时间和触发更新。
A. 水平分割　　B. 垂直分割
C. 水平分割或垂直分割　　D. 水平分割和垂直分割

19. 建立访问控制列表具有(　　)的作用。
A. 限制用户的行为　　B. 控制网络流量
C. 限制网络病毒的传播　　D. 以上 3 个选项都对

20. 参数 deny 是配置(　　)时使用的。
A. 静态路由　　B. 隧道
C. 虚拟终端　　D. 访问控制列表

二、判断题(正确的打√,错误的打×,每小题 1 分,本题共 10 分)

1. RIPv2 的跳跃计数的最大值与 RIPv1 的跳跃计数的最大值一样,不可以支持更大的网络规模。(　　)
2. OSPF 通常有 4 个版本,即 OSPFv1、OSPFv2、OSPFv3、OSPFv4。(　　)
3. copy flash: ftp:命令的作用是备份路由表到 FTP 服务器。(　　)
4. network 命令仅用于配置静态路由。(　　)
5. RIP 允许的最大跳数为 15。(　　)
6. ACL 能够提高网络访问的安全级别。(　　)
7. OSPF 数据包共有 4 种类型。(　　)
8. 命令 ipv6 unicast-routing 的作用是全局启用转发 IPv6 单播特性。(　　)
9. EIGRP 支持 IPv4、IPv6、Apple Talk 和 IPX 等多种网络层协议。(　　)
10. 标准的 ACL 使用 1～99 以及 1000～1999 之间的正整数作为表编号。(　　)

三、填空题(每空 1 分,本题共 10 分)

1. 蠕虫病毒在网络中传播的常用端口是 TCP135、________和________。
2. 目前,访问控制列表主要分为________ ACL、________ ACL 和________ ACL 三大类。
3. 如果双绞线的两端都使用 568B 接线规范,则称为________线;如果双绞线一端使用 568B 接线规范,而另一端使用 568A 规范,则称为________线。
4. 配置一条 IPv6 静态路由的命令格式是________________________________。
5. 6to4 是一种____技术。

6. 命令 ipv6 enable 的作用是____。

四、名词解析(每个名词 5 分,本题共 10 分)

1. RIPng 协议

2. GRE 隧道

五、简答题(每小题 3 分,本题共 12 分)

1. 假设路由器原来的名字是 Router1,要求将路由器的名字修改为 Router2,请写出相关的命令(注意:要写出完整的提示符)。

2. 设置路由器从普通模式进入特权模式的密文为 supervisor2018,请写出完整的提示符和相关命令。

3. 设置路由器的快速以太网接口 0/0 的 IP 地址为 11.11.11.11,并激活接口;设置串行接口 Serial 0/0 的 IP 地址为 22.22.22.22,时钟频率为 64 000Hz,并激活接口。请写出相关命令。

4. 为路由器配置 EIGRP 协议,请写出相关命令。

六、综合题（本题共 18 分）

① 如图 B-2 所示，超级终端与路由器 A 之间用什么连接线？超级终端连接线应分别接到超级终端与路由器的什么接口？两路由器之间用什么连接线？路由器与交换机之间用什么连接线？（4 分）

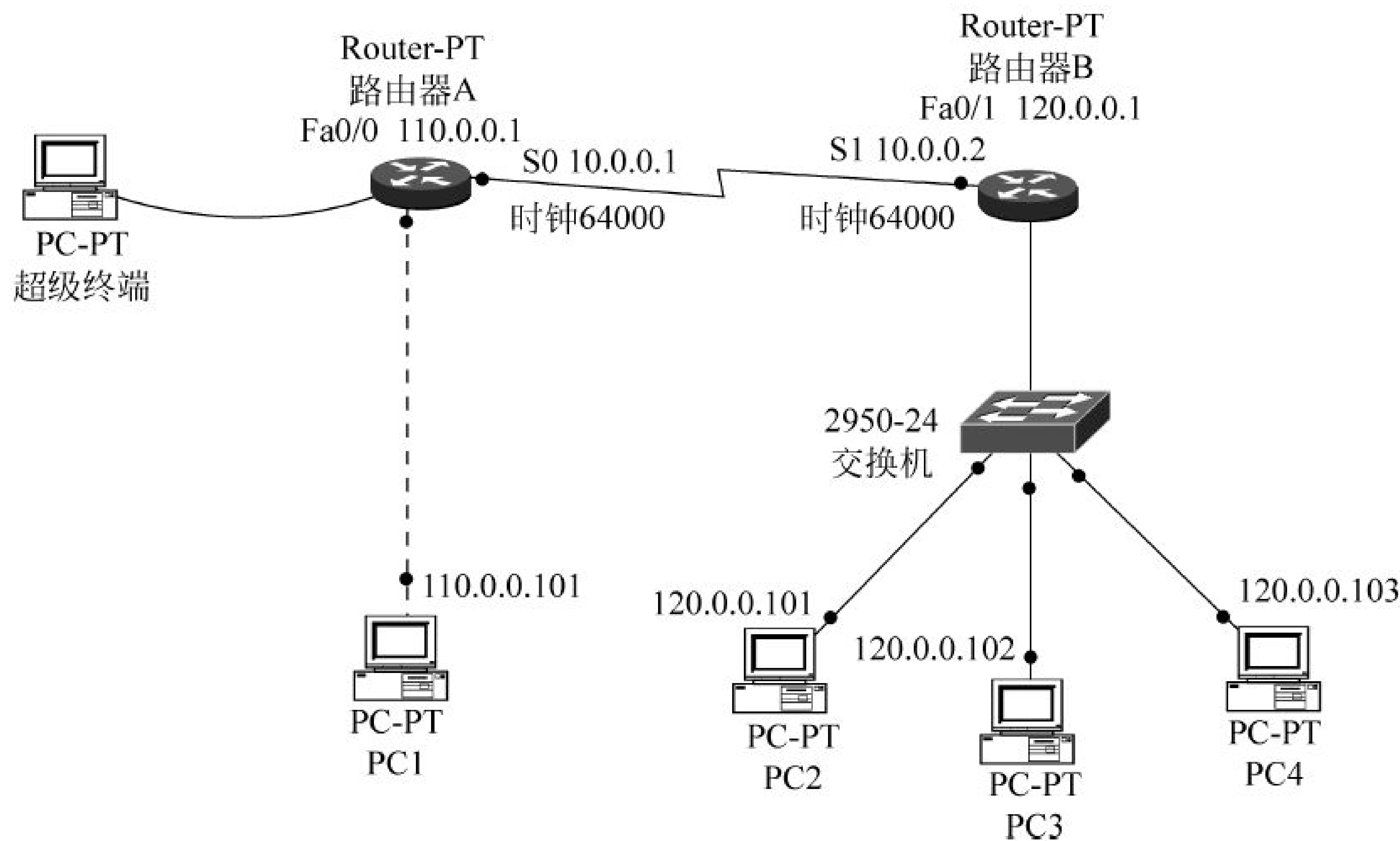


图 B-2

② 请按图 B-2 所示的网络环境配置路由器 A 串行接口 S0 和快速以太网接口的参数，并给出相关的配置命令。（4 分）

③ 请按图 B-2 配置计算机 PC1 的网络接口的参数，给出相关的配置命令或方法，并给出测试网络接口参数的方法。（4 分）

④ 如图 B-2 所示，分别给出配置路由器 A、B 工作模式为 RIPv2 的命令，并给出测试网络的连通性的相关命令。（6 分）

附录 C 常用英文缩写对照表

APPENDIX C

2B1Q	2Binary,1Quaternary 两个二进制位,一个四进制位(编码)
AAL	ATM Adaptation Layer ATM 适应层
ADSL	Asymmetric Digital Subscriber Line 非对称数字用户线路
CDV	Cell Delay Variation 信元延迟变更
CLR	Cell Loss Ratio 信元丢失比率
IDLC	Integrated Digital Loop Carrier 综合数字环路载波
AD-PCM	Adaptive Differential Pulse Code Modulation 适应微分—脉冲码调制
AL	Application Layer 应用层
AM	Amplitude Modulation 幅度调制
AMI	Alternate Mark Inversion 交替标记倒置
AN	Access Node 访问结点
ANSI	American National Standards Institute 美国国家标准协会
AP	Access Point 接入点
APS	Automatic Protection Switching 自动保护开关
ARP	Address Resolution Protocol 地址解析协议
ARQ	Automatic Repeat reQuest 自动重复请求
AS	Autonomous System 自治系统
AT&T	American Telephone & Telegraph 美国电话/电报
ATM	Asynchronous Transfer Mode 异步传输模式
ATU	ADSL Termination Unit ADSL 终端单元
AUI	Attachment Unit Interface 同轴电缆接口
AUX	Auxiliary 辅助接口
AWG	American Wire Gauge 美国线规
BDR	Backup Designated Router 备份指定路由器
BECN	Backward Explicit Congestion Notification 反向显示拥塞通知
BER	Bit-Error Rate 位误码率
BGP	Border Gateway Protocol 边界网关协议
BH	Busy Hour 高峰时
BISDN	Broadband Integrated Services Digital Network 宽带综合业务数字网

BNC	Bayonet Nut Connector 卡扣配合型连接器
BOM	Beginning Of Message 报头
BRI	Basic Rate Interface 基速接口
CAC	Connection Admission Control 连接容许控制
CAD	Computer-Aided Design 计算机辅助设计
CAE	Computer-Aided Engineering 计算机辅助工程
CAM	Computer-Aided Manufacturing 计算机辅助制造
CAP	Carrierless Amplitude Modulation 无载波幅度调制
CATV	Cable Television or Community Antenna Television 有线电视或公用天线电视
CBDS	Constant Bit Rate Data Service 不变比特率数据服务
CBR	Continuous Bit Rate,or Constant Bit Rate 连续的比特率或不变的比特率
CCITT	Consultative Committee on International Telegraph and Telephone 国际电话电报咨询委员会
CFM	Configuration Management 配置管理
CIR	Committed Information Rate 承诺信息速率
CISC	Complex Instruction Set Computer 复杂指令集计算机
CLEC	Competitive Local Exchange Carrier 竞争的本地交换载波
CLI	Command Line Interface 命令行接口
CLLM	Consolidated Link-Layer Management 统一链路层管理
CLP	Cell Loss Priority 单元丢失优先权
CMT	Connection Management 连接管理
CO	Central Office 中心局
COM	Communication 通信
COM	Continuation of Message 报文附加
COMSAT	Communications Satellite Corporation 通信卫星公司
CPE	Customer Premises Equipment 用户驻地设备
CPN	Customer Premises Node 用户驻地结点
CPU	Center Process Unit 中央处理器
CRC	Cyclic Redundancy Check 循环冗余校验
CS	Convergence Sublayer 收敛子层
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance 载波侦听多路访问/冲突避免
CSMA/CD	Carrier Sense Multiple Access with Collision Detection 载波侦听多路访问/冲突检测
CSU	Channel Service Unit 信道服务单元
DAS	Dual Attachment Stations 双附加配置工作站
DBS	Direct Broadcast Satellite 直播卫星
DCC	Data Communications Channels 数据通信信道

DCE	Data Communications Equipment 数据通信设备
DE	Discard Eligibility 丢弃合格
DHCP	Dynamic Host Configuration Protocol 动态主机协议
DLC	Digital Loop Carrier 数字环路载波
DLCI	Data-Link Connection Identifier 数据链路连接鉴定
DMT	Discrete Multitone 离散的多频声
DNS	Domain Name System 域名系统
DOJ	Department Of Justice 司法部
DR	Designated Router 指定路由器
DSLAM	DSL Access Multiplexer DSL 访问多路复用器
DSP	Digital Signal Processor 数字信令处理器
DSU	Data Service Unit 数据服务单元
DTE	Data Terminal Equipment 数据终端设备
DTP	Data Transport Protocol 数据传输协议
DTPM	Data Transport Protocol Machine 数据传输协议器
EA	Extended Address 扩展地址
ECM	Coordination Management 调和管理
ECN	Explicit Congestion Notification 显示拥塞通告
ECSA	Exchange Carriers Standards Association 交换信号标准协会
EGP	Exterior Gateway Protocol 外部网关协议
EIGRP	Enhanced Interior Gateway Routing Protocol 增强内部网关路由协议
EO	End Office 分局
EOM	End Of Message 报尾
ETSI	European Telecommunications Standards Institute 欧洲电讯标准协会
FCC	Federal Communications Commission 联邦通信委员会
FCS	Frame Check Sequence 帧校验序列
FDDI	Fiber Distributed Data Interface 光纤分布式数据接口
FDM	Frequency Division Multiplexing 频分复用
FEC	Forward Error Control 转发误码控制
FECN	Forward Explicit Congestion Notification 转发显示拥塞通告
FEP	Front-End Processor 前端处理机
FM	Frequency Modulation 频率调制(调频)
FR	Frame Relay 帧中继
FRI	Frame Relay Interface 帧中继接口
FSK	Frequency Shift Keying 移频键控(调制),频移键控(法)
FSN	Full Service Network 全服务网络
FTAM	File Transfer Access and Management 文件传输访问和管理
FTP	File Transfer Protocol 文件传输协议
FTTC	Fiber To The Curb 光纤到路边

FTTN Fiber To The Node 光纤到结点
FTTH Fiber To The Home 光纤到家
GAN Global Area Network 全局网
GEOS Geo-Synchronous Satellites 地球同步卫星
GFC Generic Flow Control 一般溢出控制
GPRS General Packet Radio Service 通用分组无线服务技术
HDLC Hign-Level Data Link Control 高级数据链路控制
HDSL High-Speed Digital Subscriber Line 高速数字用户线路
HDT Host Digital Terminal 主机数字终端
HDTV High-Definition Television 高清晰度电视
HE Header Extension 报头扩展
HEC Header Error Control 报头误码控制
HFC Hybrid Fiber/Coax 混合光纤/同轴
HIPPI High-Performance Parallel Interface 高性能并行接口
HOB Head Of Bus 总线头
HPNA Home Phoneline Networking Alliance 家庭电话线网络联盟
HRC Hybrid Ring Control 混合环控制
HSSI High-Speed Serial Interface 高速串行接口
HTTP Hyper Text Transfer Protocol 超文本传输协议
HTU-C HDSL Termination Unit-Central HDSL 终端单元—局端
HTU-R HDSL Termination Unit-Remote HDSL 终端单元—客户端
IA Intel Architecture Intel 架构
I/O Input/Output 输入/输出
IAO Intraoffice Optical Interface 局内光接口
IBM International Business Machines 国际商用机器公司
IC Integrated Circuit 综合电路
ICI Intercarrier Interface 载波间接口
ICIP Intercarrier Interface Protocol 载波间接口协议
ICMP Internet Control Message Protocol Internet 控制报文协议
IDSL ISDN Basic Access DSLs ISDN 基本访问 DSL
IEC InterExchange Carriers
IETF Internet Engineering Task Force 国际互联网工程任务组
IGMP Internet Group Management Protocol Internet 组管理协议
IGP Interior Gateway Protocol 内部网关协议
IGRP Interior Gateway Routing Protocol 内部网关路由协议
IHA Internet Home Alliance 互联网家庭联盟
IN Intelligent Network 智能网
INTUG International Trade and User Groups 国际贸易和用户群
iOS Internet Operation System 互联网操作系统

IP	Intelligent Peripheral/Internet Protocol 智能外部设备/互联网协议
IPv4	Internet Protocol version 4 互联网协议第 4 版
IPv6	Internet Protocol version 6 互联网协议第 6 版
ISDN	Integrate Services Digital Network 综合业务数字网
ISM	Industrial Scientific Medical band 工业科学医学频段
IS-IS	Intermediate System to Intermediate System 中间系统到中间系统
ISO	International Organization for Standardization 国际标准化组织
ISP	Internet Service Procider 互联网服务提供商
ISSI	Inter-Switching System Interface 内部交换系统接口
ITFS	Instructional Television Fixed Service 教育电视专用服务
ITU	International Telecommunications Union 国际电讯联盟
IWU	Internetworking Unit 网络单元
IXC	IntereXchange Carrier 内部交换电信公司
JPEG	Joint Photographic Experts Group 联合摄影专家组
LAN	Local Area Network 局域网
LAP-B	Link Access Protocol-B 链路访问协议 B
LATA	Local Access Transport Area 本地访问传输区域
LEA	Line Extender Amplifier 线延伸放大器
LEC	Local Exchange Carrier 本地交换载波
LED	Light-Emitting Diodes 发光二极管
LEOS	Low Earth Orbiting Satellite 低轨道地球卫星
LLC	Logical Link Control 逻辑链路控制
LMDS	Local Multipoint Distribution Service 本地多点分布服务
LME	Layer Management Entity 层管理实体
LMP	Layer Management Protocol 层管理协议
LOH	Line Overhead 线路管理费用
LSDB	Link State Database 链路状态数据库
LSR	Link State Request 链路状态请求
LSU	Link State Update 链路状态更新
LTE	Line Terminating Equipment 线路终结设备
LTU	Line Termination Unit 线路终端单元
MAC	Media Access Control 介质访问控制
MAN	Metropolitan Area Network 城域网
MARS	Multicast Address Resolution Server 组播地址解析协议
MDF	Main Distribution Frame 总配线架
MDS	Multipoint Distribution Service 多点分布服务
MDSL	Medium-Speed Digital Subscriber Line 中速数字用户线路
MEOS	Medium Earth-Orbiting Satellite 中地球轨道卫星
MFJ	Modified Final Judgment 修正的最终判断

MHS Message-Handling System 信息处理系统
MIB Management Information Base 管理信息库
MLD Multicast Listener Discover 组播侦听者(协议)
MMDS Multichannel Multipoint Distribution Service 多通道多点分布服务
MMF Multimode Fiber 多模光纤
MPEG Motion Picture Experts Group 运动图像专家组
MSO Multi-System Operator 多系统操作员
NAP Network Access Provider 网络访问提供商
ND Neighbor Discovery 邻居发现
NID Network Interface Device 网络接口设备
NIF Neighborhood Information Frame 邻近信息块
N-ISDN Narrowband ISDN 窄带 ISDN
NIUF North American ISDN User's Forum 北美 ISDN 用户论坛
NME Network Management Entity 网络管理实体
NNI Network-Network Interface 网间接口
NNTP Network News Transfer Protocol 网络新闻传输协议
NSAP Network Source Access Point 网络源访问点
NTIA National Telecommunications and Information Administration 国家远程通信和信息管理局
NTP Network Transport Provider 网络传输提供商
NTSC National Television System Committee 国家电视制式委员会
NTU Network Temination Unit 网络终端单元
NVOD Near Video On Demand 近距离视频点播
NVRAM Non-Volatile Random Access Memory 非易失性随机访问存储器
O/E Optical to Electrical 光电转换
OAM Operations,administration and Maintenance 操作管理和维护
OAM&P Operations,Administration,Maintenance and Provisioning 操作管理维护和供应
OC Optical Carrier 光波
OCI Optical Carrier Interface 光波接口
ONI Optical Network Interface 光网接口
ONU Optical Network Unit 光网络单元
OS Operations System 操作系统
OSI Open Systems Interconnection 开放系统互联
OSPF Open Shortest Path First 开放式最短路径优先
OTA Office of Technology Assessment 技术评价处
PA Prearbitrated 预仲裁
PCS Personal Communications Services 个人通信服务
PDH Plesiochronous Digital Hierarchy 准同步数字体系

PDU	Protocol Data Unit 协议数据单元
PES	Packetized Elementary Stream 打包的基本码流
PFM	Parameter Frame Management 参数构成管理
PHY	Physical Layer Protocol 物理层协议
PLPC	Physical Layer Convergence Protocol 物理层收敛协议
PM	Phase Modulation 脉冲调制
PMD	Physical Layer Medium Dependent 物理层中间依靠
POH	Path Overhead 路径负载
PON	Passive Optical Network 无源光网络
POP	Point Of Presence 电话接入网[站]点
POP3	Post Office Protocol version 3 第 3 版的邮局协议
POTS	Plain Old Telephone Service 普通老式电话服务
PPL	Phase Locked Loop 脉冲锁定环路
PPV	Pay Per View 有价值意见
PPP	Point-to-Point Protocol 点到点协议
PRI	Primary Rate Interface 主速率接口
PRM	Protocol Reference Model 协议参考模型
PS	Program Stream 程序流
PSTN	Public Switched Telephone Network 公用电话交换网
PT	Payload Type 有效载荷类型
PTE	Path-Terminating Equipment 路径终结设备
PTM	Packet Transfer Mode 包传输模式
PTT	Post，Telephone and Telegraph 局、电话和电报
PVC	Permanent Virtual Circuit 永久虚电路
QA	Queued Arbitrated 队列裁定
QAM	Quadrature Amplitude Modulation 正交调幅，90°相移幅度调制
QoS	Quality of Service 服务质量
QT	Queuing Technique 队列技术
RAM	Random Access Memory 随机存取存储器
RBOC	Regional Bell Operating Company 地区性贝尔营运公司
RIP	Routing Information Protocol 路由信息协议
RIPng	Routing Information Protocol next generation 下一代路由信息协议
RISC	Reduced Instruction Set Computer 精简指令集计算机
RME	Routing Management Entity 路由管理实体
RMN	Remote Multiplexer Node 远程多路复用结点
RMP	Routing Management Protocol 路由管理协议
RMS	Root Mean Square 均方根
RMT	Ring Management 时钟管理
ROM	Read Only Memory 只读存储器

SAP Service Access Point 服务访问点
SAR Segmetnation and Reassembly Sublayer 分割和重新组装子层
SAS Single Attachment Stations 单配置工作站
SCP Service Control Point 服务控制点
SDLC Synchronous Data Link Control 同步数据链路控制
SDM Space Division Multiplexing 空间分割多路复用,空分多路
SDM Security Device Manager 安全设备管理器
SDMT Synchronized DMT 同步的 DMT
SDSL Symmetric Digital Subscriber Line 对称数字用户线路
SDU Service Data Unit 服务数据单元
SLIP Serial Line Internet Protocol 串行线路网际协议
SIF Status Information Frame 状态信息帧
SMF Single Mode Fiber 单模光纤
SMS Service Management System 服务管理系统
SMT Station Management 工作站管理
SMTP Simple Mail Transfer Protocol 简单邮件传输协议
SNA System Network Architecture 系统网络体系结构
SNI Subscriber Network Interface 用户网络接口
SNMP Simple Network Management Protocol 简单网络管理协议
SNTP Simple Network Time Protocol 简单网络时间协议
SP Security Policy 安全策略
SPD Security Policy Database 安全策略数据库
SPDU Session Protocol Data Unit 会话层协议数据单元
SPT Shortest Path Tree 最短路径树
SRF Status Report Frame 状态报告帧
SS7 Signaling System Number 7 号信令系统
SSH Secure Shell 安全外壳协议
SSP Service Switching Point 服务交换点
STB Set-Top Box 置顶盒
STP Shielded Twisted Pair 屏蔽双绞线
STV Sprint Telecommunications Venture sprint 电讯风险
SVC Switched Virtual Circuit or Signaling Virtual Circuit 交换式虚电路或发信号虚电路
TA Trunk Amplifier 主干放大器
TA1996 Telecommunications Act of 1996 1996 电讯法令
TC Transmission Convergence 转发收敛
TCP Transmission Control Protocol 传输控制协议
TDD Time Division Duplexing 时分复用
TDMA Time Division Multiple Access 时分多路访问

TELNET	Telecommunication Network 远程通信网络
TFTP	Trivial File Transfer Protocol 简单文件传输协议
TP	Transaction Processing 事务处理
TRT	Token Rotation Timer 令牌旋转计时器
TS	Transport Stream 传输流
TTL	Time To Live 生存时间
TTRT	Target Token Rotation Timer 目标令牌旋转计时器
TVT	Transmission Valid Timer 正确传输计时器
UAWG	Universal ADSL Working Group 通用 ADSL 工作组
UDP	User Datagram Protocol 用户数据报协议
UNI	User Network Interface 用户网络接口
UTOPIA	Universal Test and Operations Physical Interface for ATM ATM 通用测试和操作物理接口
URL	Uniform Resource Locator 统一资源定位器
UTP	Unshielded Twisted Pair 非屏蔽双绞线
VBR	Variable Bit Rate 变量位率
VCI	Virtual Channel Identifier 虚通道鉴定
VDSL	Very High-Bit Rate Digital Subscriber Line 非常高位率数字用户线路
VDT	Video Dial Tone 视频拨号音
VIP	Video Information Provider 视频信息提供商
VoD	Video on Demand 视频点播
VPI	Virtual Path Identifier 虚路径鉴定
VRP	Virtual Reality Platform 虚拟现实平台
VRP	Versatile Routing Platform 通用路由平台(华为操作系统)
WAN	Wide Area Network 广域网
WCA	Wireless Cable Association 无线联盟
WDM	Wavelength Division Multiplexing 波长分割多路转换器
WiFi	Wireless-Fidelity 无线网络
WLAN	Wireless Local Area Networks 无线局域网
WWW	World Wide Web 万维网
XC	Cross Connect 交叉连接

参 考 文 献

[1] Henry Benjamin. CCNP 实战指南：路由[M]. 刘忠庆，译. 北京：人民邮电出版社，2002.
[2] 潘冰，陈焱. CCNA 实用培训教程[M]. 北京：清华大学出版社，2003.
[3] Kenneth D Reed. TCP/IP 基础[M]. 7 版. 北京：电子工业出版社，2004.
[4] Kenneth D Reed. 网络互联设备[M]. 7 版. 北京：电子工业出版社，2004.
[5] 冯昊，黄治虎，伍技祥. 交换机/路由器的配置与管理[M]. 北京：清华大学出版社，2005.
[6] 宁芳露，杨旭东. 网络互联及路由器技术教程与实训[M]. 北京：北京大学出版社，2005.
[7] 梁广民，王隆杰. 网络设备互联技术[M]. 北京：清华大学出版社，2006.
[8] 张海涛，王鹰，陈绮，等. 下一代网络路由技术[M]. 北京：机械工业出版社，2006.
[9] 甘刚，孙继军. 网络设备配置与管理[M]. 北京：中国水利水电出版社，2006.
[10] H3C. H3C 网络学院教程[M]. 北京：杭州华三公司，2007.
[11] 张保通，李伟红. 网络互联技术——路由、交换与远程访问[M]. 2 版. 北京：中国水利水电出版社，2008.
[12] 高峡. 网络设备互联学习指南[M]. 北京：科学出版社，2009.
[13] Mark A Dye，Rick McDonald，Antoon W Rufi. 思科网络技术学院教程：网络基础知识[M]. 思科系统公司，译. 北京：人民邮电出版社，2009.
[14] Rick Graziani，Allan Johnson. 思科网络技术学院教程：路由协议和概念[M]. 思科系统公司，译. 北京：人民邮电出版社，2009.
[15] 徐宇杰. IPv6 深入分析[M]. 北京：清华大学出版社，2009.
[16] 汪双顶，姚羽. 网络互联技术与实践教程[M]. 北京：清华大学出版社，2009.
[17] 施晓秋，张纯容，金可仲. 网络工程实践教程[M]. 北京：高等教育出版社，2010.
[18] 杨云江，高鸿峰. IPv6 技术与应用[M]. 北京：清华大学出版社，2010.
[19] 王书明，韩永辉，等. 网络设备与互联[M]. 北京：清华大学出版社，2010.
[20] 徐良贤，等. 计算机网络与因特网[M]. 北京：机械工业出版社，2010.
[21] 贾卓生. 互联网及其应用[M]. 北京：机械工业出版社，2011.
[22] 吴建胜，孙良旭，张玉军. 路由交换技术[M]. 北京：清华大学出版社，2011，
[23] 杨国良，李阳春，伍佑明. IPv6 技术、部署与业务应用[M]. 北京：人民邮电出版社，2011.
[24] 甘刚. 网络设备配置与管理[M]. 北京：人民邮电出版社，2011.
[25] 刘京中，邵慧莹. 网络互联技术与实践[M]. 北京：电子工业出版社，2012.
[26] 骆耀祖，杨波. 路由与交换实用技术[M]. 北京：机械工业出版社，2012.
[27] Regis Desmeules. Cisco IPv6 网络实现技术(修订版)[M]. 2 版. 王玲芳，张宇，李颖华，孙向辉，译. 北京：人民邮电出版社，2013.
[28] Rick Graziani. IPv6 技术精要[M]. 夏俊杰，译. 北京：人民邮电出版社，2013.
[29] Joseph Davies. 深入解析 IPv6. [M]. 汪海霖，译. 北京：人民邮电出版社，2014.
[30] 刘晓辉，刘险峰，王雪梅. 网络硬件设备完全技术宝典[M]. 北京：中国铁道出版社，2013.
[31] 张国清，路由技术(IPv6 版)[M]. 北京：电子工业出版社，2014.
[32] 姜大庆，吴强，杨明胜. 网络互联及路由器技术[M]. 2 版. 北京：清华大学出版社，2014.
[33] 张纯容，施晓秋，刘军. 网络互联技术[M]. 北京：电子工业出版社，2015.
[34] 田果，彭定学. 趣学 CCNA——路由与交换[M]. 北京：人民邮电出版社，2015.
[35] Andrew S Tanenbaum. Computer Networks(Third Edition)[M]. Prentis Hall，1996.
[36] Douglas E Comer. 用 TCP/IP 进行网际互联第 1 卷：原理、协议与结构[M]. 林瑶，蒋慧，杜蔚轩，译. 北京：电子工业出版社，2001.

图书资源支持

感谢您一直以来对清华版图书的支持和爱护。为了配合本书的使用，本书提供配套的资源，有需求的读者请扫描下方的“书圈”微信公众号二维码，在图书专区下载，也可以拨打电话或发送电子邮件咨询。

如果您在使用本书的过程中遇到了什么问题，或者有相关图书出版计划，也请您发邮件告诉我们，以便我们更好地为您服务。

我们的联系方式：

地　　址：北京海淀区双清路学研大厦 A 座 707

邮　　编：100084

电　　话：010－62770175－4604

资源下载：http://www.tup.com.cn

电子邮件：weijj@tup.tsinghua.edu.cn

QQ：883604（请写明您的单位和姓名）



书圈

用微信扫一扫右边的二维码，即可关注清华大学出版社公众号“书圈”。